

MANAGEMENT SOFTWARE

VSOIP LITE 3.1

USER MANUAL

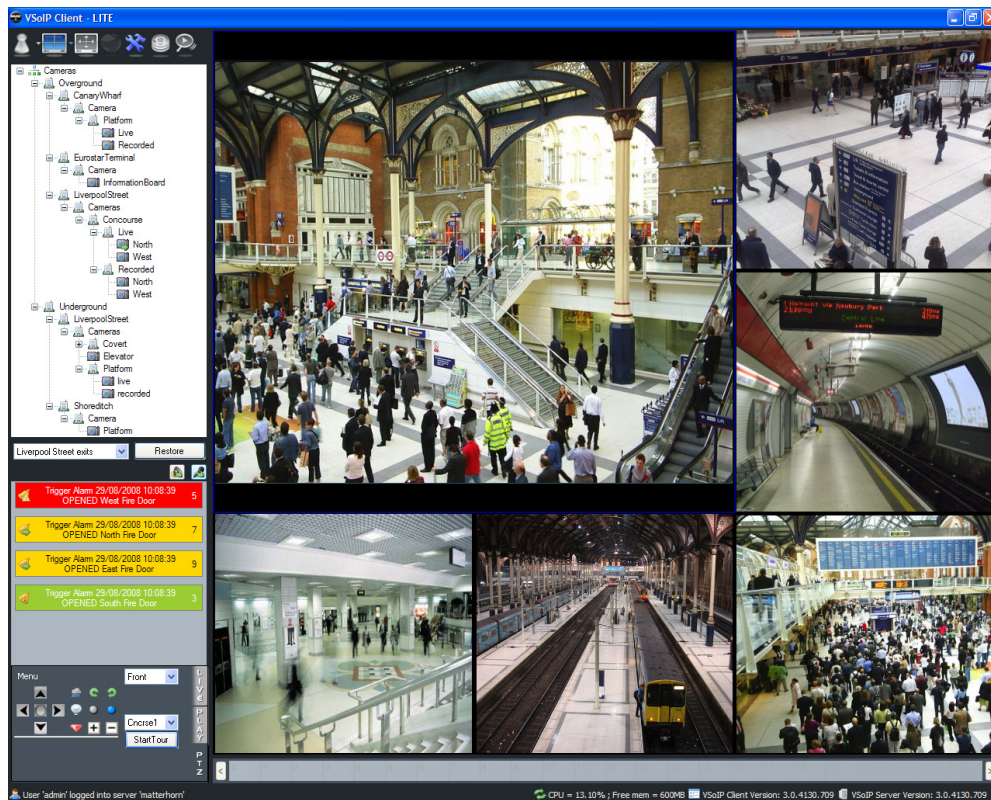


Table of Contents

About This Guide	5
Safety Terms	5
1 System Overview	6
System Components	6
Surveillance Suite Architecture	6
IP Camera and DVR Configuration	6
System Environment	6
Network Traffic	6
Infrastructure	7
Configuring Stream Settings	7
System Software	8
Shutting Down the Computer	9
2 Installing VSoIP Lite.....	10
Introduction.....	10
Prerequisites.....	10
Hardware.....	10
Operating System	11
Additional mandatory software	11
Before Installing VSoIP Lite.....	12
Operating System Settings	12
Networking Settings	12
Installing VSoIP Lite	14
Upgrading VSoIP Lite	14
Upgrading VSoIP Lite's Recording Streams.....	14
Uninstalling VSoIP Lite	15
Uninstalling for Upgrade Purposes.....	15
Performing a Complete Uninstall.....	15
3 Client/Server Configuration	17
Getting Started.....	17
User Configuration.....	18
Changing User Passwords.....	18
Device Configuration	19
Adding Devices	19
Configuring Devices using the Web Interface	24
Deleting Devices	25
Configuring Video Sources.....	26
Configuring Triggers.....	27
Configuring Pan-Tilt-Zoom Capabilities.....	28
Configuring Audio	29
Communicating Using Audio.....	30
Configuring Sequences	31

4 Using VSolP Lite to Monitor your Site	32
Working with Live Video and PTZ.....	32
Specifying Video Pane Layout.....	33
Starting and Stopping Live Video	34
Using Digital Zoom	35
Taking a Snapshot of Live Video	36
Control of Pan-Tilt-Zoom	37
Viewing Sequences	38
Working with Alarms	40
Overview of Alarm Display	40
Viewing Properties of an Alarm.....	40
Acknowledging an Alarm.....	41
Closing an Alarm.....	42
The Audit Trail	43
Audit Trail Management	43
 5 Recording with VSolP Lite	 44
Recording Camera Footage	44
Recordings Storage Overview	44
What Happens When a Partition Becomes Full?	45
Creating a Recording Job.....	45
Using Stream Sampling to Reduce Required Storage Space.....	46
Playing Back Recorded Video	48
Discovering Recorded Footage.....	48
Playing Back Recorded Footage.....	50
Using Digital Zoom	51
Taking a Snapshot of Recorded Video	52
Editing Recording Jobs	52
Deleting/Disabling Recordings	53
Synchronising Playback of Recorded Footage	54
Exporting Recorded Video.....	55
VSolP Export Player.....	55
 6 System Administration	 56
Restoring Factory Defaults	56
Viewing System Information	57
Default Settings	58
 Appendix A Maintenance Information.....	 60
Opening a Command Prompt in Microsoft Windows	60
Opening the Run dialog.....	60
Finding out the IP Address of Your Computer	60
Determining PC Port Usage	61
Windows Events – Using the Event Viewer.....	62
Displaying Hidden or System Files.....	62
Configuring Application Log to Overwrite Oldest Entries.....	64
Viewing Windows Services List.....	65
Checking Connectivity of a Networked Device or Computer.....	66
Troubleshooting	67
Providing Technical Support Information.....	68
Specifying the Logging Level	70
 Appendix B Supported Devices.....	 71

Appendix C Specific Device Considerations.....	73
Adding ZV-S306 and ZN-D2024 Devices to VSoIP Lite	73
Adding DRH-DVD and DR4H Lite DVRs	73
Index.....	74

About This Guide

VSolP Lite's all-in-one architecture is based on one standard Windows PC acting as an IP video stream recording service, surveillance system manager and live video, PTZ control, play back and recorder control client for Windows.

You may have received VSolP Lite free when you purchased a GANZ device. This free version contains an embedded Networked Video Recorder which provides access to four recording streams.

You can upgrade this free version to have 16 recording streams. For information on how to do this, see "Upgrading VSolP Lite" on page 14.

Safety Terms

These terms may appear in this manual:

Table 1 Safety terms

Caution	Cautions identify conditions or practices that may result in below optimum system performance
Warning	Warnings identify conditions or practices that could result in equipment damage or serious personal injury.

Chapter 1 – System Overview

This chapter contains information on the following:

- System Components
- System Environment
- Shutting Down the Computer

VSolP Lite's all-in-one architecture is based on one standard Windows PC acting as an IP video stream recording service, surveillance system manager and live video, PTZ control, play back and recorder control client for Windows.

Caution: When turning off the computer, it is **essential** to shut it down properly — incorrect shutdown could affect the recording element of VSolP Lite and risk loss of previously recorded footage, or recorder system failure. For details, see “Shutting Down the Computer” on page 9.

This system is a complex one with Ganz supplying differing hardware with different feature sets and characteristics. In such systems the adherence to standards is the route relied on to make the overall system work.

The system architecture is based on an Internet Protocol (IP) network — all communication is performed over IP networks — and the surveillance suite software relies on Microsoft Windows technologies.

System Components

VSolP Lite consists of a combined client/server/Networked Video Recorder (NVR). These components are installed during installation and work seamlessly together.

Surveillance Suite Architecture

When the system components are installed on computer hardware and given access to compatible IP cameras and networked digital video recorders, the components act together to form a surveillance system.

IP Camera and DVR Configuration

Please note that devices should be configured in the manner indicated in the list at system installation time. Device configuration support is not provided by the surveillance software suite.

System Environment

The system makes use of Internet Protocol based computer networks. The construction of such networks is beyond the scope of this document however the network design must take into full consideration the large quantity of data transferred across networks by surveillance systems.

It is useful however to have a high level discussion of the major areas that should be addressed when designing such a network and choosing the communication parameters of the IP cameras and networked digital video recorders attached to the network.

Network Traffic

Video streamed from IP cameras and networked digital video recorders is the major configurable source of traffic on the network. The quantity of data traffic from each source accumulates as it is consumed by increasing numbers of devices.

Furthermore, since the integrated NVR replays recorded network streams, the amount of data traffic generated is the same as that of the original recorded stream. Multiple playback sessions of the same recorded stream result in an accumulation of data traffic in line with the number of playback sessions.

Infrastructure

When planning system infrastructure, you should take the following into account:

- Cable connections to a typical network switch device have maximum rates of 100 or 1000 megabits per second.
- Network connection between a device and a network switch can be:
 - Half-duplex – they can either send or receive traffic at any given moment.
 - Full-duplex – they can send and receive traffic at the same time.
- A network connection might have traffic from:
 - A single IP camera or networked digital video recorder (DVR) only.
 - IP cameras and networked DVRs.
- There may be non-surveillance network data on the same network.
- Multicast traffic may help reduce bandwidth requirements. However, it may not be supported by the surveillance suite components.
- A network time server. The presence of a hardware or software based time server is a mandatory requirement. All IP cameras, encoders, networked digital video recorders, server and client computers should obtain their base time from the network time server. For evidential purposes, the central time server should synchronise itself with an external real-world time source. Where there are multiple surveillance site locations, local time servers in each location should provide time to the site. Each local time server should coordinate with the same external real-world time source.

Configuring Stream Settings

When configuring IP camera and Networked DVR stream settings, you should consider the following:

- Generally more traffic is generated by:
 - High resolutions.
 - High bitrates.
 - High frame-rates.
 - High frame-rate MJPEG streams, which generally tend to generate more traffic than high frame-rate MPEG4 or H.264 streams of the same resolution.
- More traffic is generated by MJPEG by high frame quality / low compression factor.
- More traffic is generated by MPEG4 or H.264 by:
 - High I-frame quality.
 - Excessively high P-frame quality.
 - Low P-frame frequency/high I-frame frequency.
 - Type of scene observed by camera(s): e.g. more data traffic is generated by: PTZ cameras that move through tours of presets, or are frequently moved; noisy feeds from analogue cameras; night-time viewing and automatic gain causing noise, scene subject to motion – crowd scenes, busy roads, in-vehicle safety cameras, etc.
- Using H.264/AVC (MPEG4-part10) encoded video network streams can achieve equivalent video quality to MPEG4-part2 encoded video network streams at lower bandwidth. Consider using H.264 encoding for more efficient use of bandwidth particularly when using mega-pixel video sources.

Note: H.264 can require more CPU power to decode than the equivalent stream encoded in MPEG4. Please consider this when interpreting PC specification requirements.

- Careful infrastructure planning will lead to an overall surveillance system that can be relied on. It is important to consider any network links that are heavily loaded by data traffic.
- It is also worth noting that when viewing live video from IP cameras and networked DVRs on a switched network, data is normally routed directly from the IP camera or networked DVR to the software viewing that camera or networked DVR, i.e. it is not received by the server component and then forwarded on to the viewing clients.
- Some IP cameras allow for different streaming rates, depending on which encoder within the camera is connected. One use of such a facility is to have one encoder on the IP camera set to typical live view settings and another encoder in the same camera set to typical recorder settings.
- Mega-pixel cameras require considerable care when deployed within a surveillance system. They can generate considerable traffic, due to their high resolution when used at 25 or 30 frames per second and when using MJPEG. The client software component will consume more PC resources than with a CIF/SIF resolution stream and thus either the specification of the PC should be revised in light of the higher decode and rendering requirements, or the number of concurrently displayed streams should be reduced, or both. If the integrated VSoIP Lite NVR is used to record high-definition, mega-pixel network streams, this puts a large load on the recorder, consuming a larger percentage of the available network connection bandwidth and consuming more storage space per second than CIF and 4CIF resolution streams.
- Predicting network traffic can be difficult so it is highly recommended that a safety margin be built in to accommodate sudden bursts of higher than average data traffic caused by a faulty camera, or similar.

System Software

The surveillance suite components are designed to run under the recommended operating system. It is assumed that the operating system installed on computer hardware is that as installed by the computer manufacturer or installed from a genuine copy of the Windows installation media.

Caution: Anti-virus, anti-spyware and software firewall products should not be installed on surveillance computers.

No additional software other than that described as prerequisites for the various surveillance system components should be installed. Adding additional software could have unforeseen impact on the satisfactory performance of the system.

It is common for IT personnel to make changes to various aspects of Microsoft Windows such as locking down certain features or applying various operating system group policies. These types of changes are not supported by the surveillance software components.

Microsoft's in-built automatic update feature should be disabled. Instead, updates to the operating system should be carried out prior to installing the surveillance software, and then during planned system maintenance. If automatic updating is enabled unexpected behaviour such as setting changes and unplanned system restarts might occur.

It is important to update all operating system device drivers, particularly for network and graphic adapters; it is best to use the latest drivers available from the computer manufacturer. If you find that the computer manufacturer uses hardware from a third party, please be certain that using the third-party's driver is appropriate — often computer manufacturers obtain specially crafted variants of the third party's hardware making the usual driver from the third party less than optimal, or completely incorrect.

All surveillance suite software components use Microsoft's .Net framework. This must be installed on all computers. The setup program for the surveillance software will attempt to install the appropriate version of the .Net framework from Microsoft's web-servers if it is not detected on the computer.

VSoIP Lite uses Microsoft's Direct-X. This must be installed prior to running VSoIP Lite, and can be obtained directly from Microsoft.

VSolP Lite also uses Microsoft's SQL Express 2005 database management system. This must be installed on the computer on which VSolP Lite is installed. The setup program for VSolP Lite will attempt to install the appropriate version of the SQL Server 2005 Express if it is not detected on the computer.

Caution: It is recommended that the SQL Express 2005 database management system uses its default values. It should not be secured in a way that prevents VSolP Lite from creating or accessing databases. SQL Express should only manage those databases added by the VSolP Lite software.

Shutting Down the Computer

There may be occasions when you need to shut down the computer whilst VSolP Lite is recording.

Caution: Incorrectly shutting down the recorder could risk loss of previously recorded footage, or recorder system failure.

The recorder continuously writes to storage media whilst operating. If the computer running the recorder needs to be disconnected from the utility power, or if the connection to a storage system is to be removed, the operating system **must** be shut down as follows:

- On the computer running VSolP Lite, use the Start menu>Shutdown shortcut, OR
- Press the [CTRL], [ALT] and [DEL] keys simultaneously, then choose the Shut Down option.

Note: An Uninterruptable Power Supply (UPS) system must be installed to prevent system corruption due to power loss. Please see "Prerequisites" on page 10.

Warning: If you do not have the necessary privileges to shut down the computer yourself then you **MUST** refer the matter to a user with the necessary authority to do so. **DO NOT** switch off the power supply to the computer as a means of shutting it down. To do so could result in irrecoverable recordings and potentially a partially or fully corrupted system, liable to fail either immediately on restarting or at some time in the future.

Chapter 2 – Installing VSoIP Lite

This chapter contains information on the following:

- Prerequisites
- Before Installing VSoIP Lite
- Installing VSoIP Lite
- Upgrading VSoIP Lite

Introduction

VSoIP Lite is a Microsoft .Net framework-based application for Microsoft Windows operating systems. It is designed to provide access to surveillance resources such as IP cameras. VSoIP Lite software consists of three integrated subcomponents: the server, the client and VSoIP Lite NVR.

The computer running VSoIP Lite should be a graphics workstation grade high powered 32- or 64-bit PC, running a 32 bit operating system.

Prerequisites

The following hardware and software components are required to run VSoIP Lite.

Hardware

Caution: It is highly recommended that you consider the different demands of the bit-rates, resolutions, frame rates, levels of compression and codec types of the system you are implementing when compared with this specification to ensure that your own system has the system performance that matches the demands it is likely to make. In addition, it is wise to add a safety overhead in addition to this to accommodate operating system efficiency changes over time.

- Processor: 32 or 64 bit architecture CPU (e.g 32 bit Intel Quad Core Processor (or better)) 2.4Ghz.
- Processor: Intel I-7 2.8ghx or greater
- CPU Cooling: High performance Active Heatsink/Fan Combination.
- Motherboard: Intel P55 Chipset
- Operating System: see "Operating System" below.
- Operating System Disk: 500Gb High performance SATA 7200rpm or greater.
- System Memory: 4GB Total of 1333MHZ DDR3 NON-ECC DIMMs 4 x 1GB.
- Optical Drive: DVD/CDRW Combo Labelflash 8x or greater.
- Graphics: Nvidia 9800GT 512MB cache PCI-e 1x.
- Integrated RAID Controller: LSI AMCC -9650SE High Performance RAID Controller, All RAID levels Supported, Max of 8 drives.
- Removeable Disk: 5 x Removeable high Performance SATA RAID Enabled Disk Drives 7200rpm -Hot Swap Capable.
- Additional Disk: 1 x additional Fixed Disk for RAID Array.

Caution: In some graphics systems, there is a limit to the maximum number of separate areas of video on-screen that can be supported at the same time, even if they have the two types of hardware enabled acceleration. This limitation appears to a user as if no more than a fixed number of players can show video, i.e. for those video areas that are not displayed, the application otherwise appears as if the video is being displayed. In this case stopping video which is being displayed in one player causes a player that was not showing video to display video. This is not a defect in the application, rather this is a limitation of the graphics system hardware in use.

- Uninterruptable Power Supply (UPS) system

To prevent system corruption due to power loss, a UPS system must be installed. This should be of a type that shuts down the operating system automatically if the utility power does not resume before the UPS power fails.

To prepare for this possibility, the computer's power-on settings, operating system, and the UPS system should be configured so that the computer is powered on and the operating system is automatically rebooted as soon as utility power is restored.

Operating System

Windows XP Professional – service pack 3, or greater, is recommended.

Note: VSolP Lite has been tested and verified on Windows 7 32-bit systems. Installation **must** be carried out as Administrator. To run the program, you must right-click VSolP Lite in the Start menu and select "Run as Administrator".

VSolP Lite is compatible with Windows 7 64-bit systems.

Note: Certain ports must be opened for VSolP Lite to operate correctly. For more details see "Firewalls and Port Usage" on page 12.

Caution: In geographical regions where several calendar types are used, please ensure that your regional Date/Time setting is set to use the Gregorian calendar.

Additional mandatory software

- Windows Installer 3.1
- Microsoft .Net Framework 3.5 SP1 or greater (includes .Net frameworks 1.1, 2.0, 3.0 and 3.5). No configuration of the .Net Framework is required.
- Microsoft SQL Server 2005 Express Edition, Service Pack 2 must be installed followed by Service Pack 3. Any required configuration of the SQL Server should occur following the installation of the client/server, once the database for the client/server has been created.

Note: These components are automatically downloaded from Microsoft during the installation process if not present at install time. They are also available from Microsoft's website as a download. Microsoft frequently redesigns its websites therefore an Internet download link is not provided. Instead we recommend that you use Google or another search engine to find the download links for the mandatory software. On examining the search results, please ensure that the download source is Microsoft.

- Microsoft Direct-X 9.0c (March 2009). See "Direct-3D Hardware Support and Microsoft Direct-X 9.0c or above" on page 13 for more information on Direct-X.
- Microsoft Internet Explorer 8 or later.

Before Installing VSoIP Lite

Operating System Settings

The PC should have the operating system installed either by the computer manufacturer or from the operating system installation media. The computer is assumed not to be the member of any Windows network domain.

Note: Changes to the operating system settings, such as changing the global policies relating to rights and permissions, are discouraged. These notes assume that the operating system is set up in a freshly installed state.

A local user account should be added. This should be a member of the local administrator group. Software installation, .Net installation and Direct-X installation, and all maintenance should be carried out as this local user with local administrative rights.

To prevent unscheduled system restarts, switch off the automatic Windows update feature. Updates to the Windows operating system should be carried out as part of scheduled system maintenance.

Networking Settings

Note: Ensure that your network card driver version is the latest available from either the card manufacturer or the computer system manufacturer. Network driver issues at high sustained network load can cause packet loss. This shows up as video corruption and if disruption is sustained, this could cause video disconnection.

- Specify the network settings for the PC and make sure that the PC network connection is enabled and connected. Check this by opening a command prompt and running the `ipconfig` Windows command-line utility, (see Appendix A, "Maintenance Information").

Caution: The surveillance system is designed to work in systems where there is a single active network connection. Multiple network cards require further configuration and so are not recommended. The surveillance system is designed to bind to the highest priority (default) network interface. If the system uses a connection other than the intended one, use the operating system's network connection tool to disable all connections other than the one intended to be used, or if other connections are required, e.g. for a NAS network, then use the Advanced Settings dialog of the Network Connections tool to specify that the network used for surveillance video is the top most in the connection order.

- The use of the Dynamic Host Control Protocol (DHCP) in the surveillance site is not recommended, as the server will be unable to locate devices if their IP address are reassigned. We recommend that static IP addresses are used at all times.

Firewalls and Port Usage

For best performance, simplicity of setup and easy maintenance, it is recommended that a dedicated firewall protects the entire network rather than firewall software running on the client/server PC.

Any local software firewalls should either be disabled, or carefully configured so as not to prevent VSoIP Lite from contacting the licensing server. Also, any hardware firewall on the LAN should be configured to allow appropriate network access to the PC on which VSoIP Lite is executing. Some local, software-based firewalls block incoming/outgoing traffic solely on a port number basis. Others block ports to all but explicitly defined applications.

Table 5 VSoIP Lite port usage

Application	Role	Default Path	Port Number	Note
Setup.exe	VSoIP Lite installer	installation media	80/TCP	The bootstrap installer for VSoIP Lite
MSI file	VSoIP Lite installer	installation media	80/TCP	The main installer for VSoIP Lite
VSoIPLite.exe	Application	C:\Program Files\GANZ\VSoIP Lite	7002/TCP	VSoIP Lite application

Note: Blocking the required ports and/or not allowing VSoIP Lite and related applications to use the network can prevent successful installation, activation or execution of VSoIP Lite. The port information and network transport for all IP cameras and encoders that are be controlled and viewed should be added to the firewall rules.

Additional Security Software

It is not advisable to execute the following on the PC unless the impact of their execution is considered carefully:

- Anti-virus
- Anti-spyware
- Software firewall

Direct-3D Hardware Support and Microsoft Direct-X 9.0c or above

To ensure maximum performance, the VSoIP Lite PC requires an excellent graphics sub-system. The minimum requirement is a graphics sub-system capable of hardware accelerated Direct 3D rendering. You should have also installed the latest released graphic drivers either from the graphics sub-system manufacturer or from the PC manufacturer.

Caution: When using MegaPixel cameras or encoders, the resolution of the rendered image might exceed the Direct -X 3D capabilities of the graphics adapter or driver. Where this occurs, the displayed image will be missing regions of the actual image being sent from the camera and can also be distorted. This is not a fault of the software but is a limitation of the graphics sub-system. Please ensure that the graphics adapter you select can render textures on a Direct-X surface equal to or greater than the resolution of the mega-pixel source.

Note: Some graphic sub-systems are modified to work in the PC manufacturer's hardware.

Use Direct-X diagnostics to determine which version of Direct-X the VSoIP Lite PC is using, and whether or not the graphics sub-system is able to support Direct 3D, as follows:

- 1 From the Windows Start menu, select Run.
- 2 In the Run dialog, enter **dxdiag**.
- 3 On the System tab, find the System Information entry for Direct-X version. Check this is 9.0c or a higher revision number.

On the Display tab, find the Direct 3D Acceleration entry and ensure that it is enabled. If either the version or 3D support is unsatisfactory, the system will be unable to run VSoIP Lite.

Installing VSoIP Lite

This section explains how to install VSoIP Lite for the first time on your computer.

- 1 Log in to the computer using the user name of the local user with administrative level privileges.
- 2 Double-click the setup.exe file to start installation.

The VSoIP Lite installer program setup.exe automatically examines the local system for the .Net Framework, SQL-Express, Direct-X and Windows Installer 3.1. If these are not present, or earlier versions are installed, the installer program automatically connects to Microsoft's servers over the Internet and downloads the correct versions of the software.

- 3 After accepting the terms and conditions, you are prompted to specify the name and size of the recording partitions that will be used to store recordings. You can accept the defaults, or change the names, locations and sizes to suit your system.

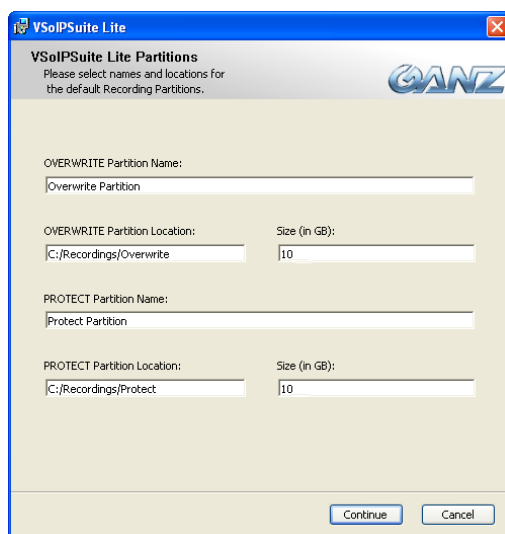


Figure 1 Setting up recording partitions

For detailed information on setting up recording partitions, please see “Recordings Storage Overview” on page 44.

- 4 Click Continue to carry on with the installation.

Caution: When installation is complete, you must restart the PC to ensure that the integrated NVR starts correctly.

Upgrading VSoIP Lite

This section explains how to increase the number of recording streams accessible by VSoIP Lite.

Upgrading VSoIP Lite's Recording Streams

You may have received VSoIP Lite free when you purchased a GANZ device. This free version contains an embedded Networked Video Recorder which provides access to 4 recording streams.

You can upgrade this free version to have 16 recording streams. Contact your supplier for details on how to purchase an upgrade. Once you have bought an upgrade for your current version of VSoIP Lite, you need to activate it, as follows:

- 1 From the Start menu, select VSoIPSuite Lite, then VSoIPSuite License Helper.

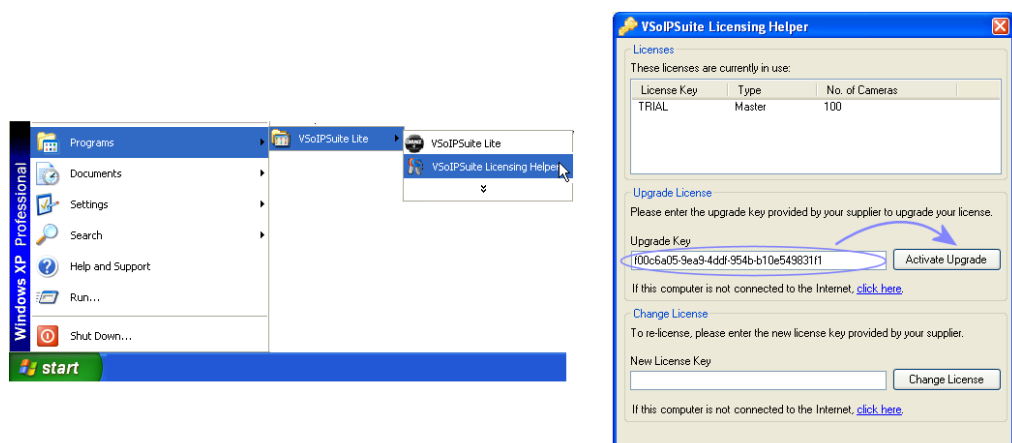


Figure 2 Activating an upgrade of VSOIP Lite

- 2 Enter the upgrade license number in the Upgrade Key box.

Caution: Take care not to add the upgrade license in the New License Key box.

- 3 Click Activate Upgrade.
- 4 Restart the PC. If this step is not carried out the recorder will continue to be limited to four recording streams until the PC is restarted. Following PC restart, the recorder is limited to recording 16 streams.

If activation fails, see “Installing VSOIP Lite”, above, for possible reasons.

Uninstalling VSOIP Lite

There may be two situations where you wish to uninstall VSOIP Lite:

- You want to uninstall so that you can upgrade to a newer version of VSOIP Lite. In this case you want to keep your current configuration to use with the new version.
- You want to completely remove all applications, data, recording data and database entries.

Uninstalling for Upgrade Purposes

To uninstall the current version of VSOIP Lite to enable you to install a newer version:

- 1 Close the VSOIP Lite application.
- 2 Stop the VSOIP Lite Recording Server. This is displayed as the Video Services service. See “Viewing Windows Services List” on page 65 for information on how to do this.
- 3 From the Start menu, select VSolPSuite Lite>Uninstall VSOIP Lite.

Note: Using this uninstall method removes the application but leaves recording data and database entries intact.

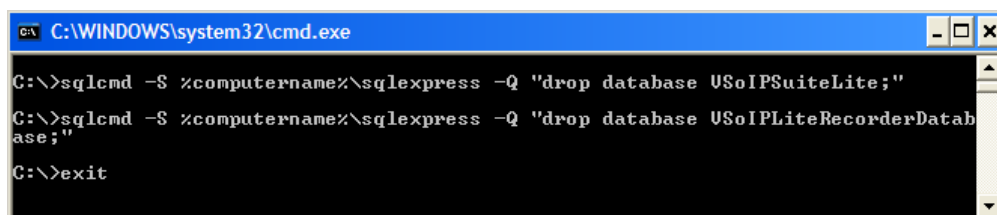
Performing a Complete Uninstall

This method removes not only the application, but also all data, recording data and database entries.

- 1 Close the VSOIP Lite application.
- 2 Use the Start menu item to remove VSOIP Lite.
- 3 Reboot the PC.
- 4 Remove the following folders and their contents:
 - C:\Documents and Settings\All Users\Application Data\GANZI\VSolPLite
 - C:\Documents and Settings\All Users\Application Data\CSDataStorage

- The folders you specified for partitions during installation. By default this is set to C:\Recordings
- 5 Open a command prompt window. From the Start menu, select Run, or hold the Windows key and press R. Type cmd in the Open box, then click OK.
 - 6 In the Command Window type the following commands, and press the Enter key at the end of each line.

```
sqlcmd -S %computername%\sqlexpress -Q "drop database  
CSServicesDatabase;"
```



The screenshot shows a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.exe". The command prompt displays the following commands and their output:

```
C:\>sqlcmd -S %computername%\sqlexpress -Q "drop database USolPSuiteLite;"  
C:\>sqlcmd -S %computername%\sqlexpress -Q "drop database USolPLiteRecorderDatabase;"  
C:\>exit
```

Figure 3 Removing VSolP Lite databases

- 7 If you have upgraded VSolP Lite to have 16 channels, you may also want to locate and delete the VSolP NVR upgrade licence. This is not an essential step but you may want to delete the licence to ensure complete deletion of all program elements.

The location of the licence varies depending on the operating system you are using:

- Windows XP:
C:\Documents and Settings\All Users\Application
Data\CBC_Europe\VSolPSuite\VSolPRecorderLicense.rai
- Windows Vista/Windows 7:
C:\ProgramData\CBC_Europe\VSolPSuite\VSolPRecorderLicense.rai

Note: Licence files may be hidden on your system. To view them, you must display hidden files and folders. For information on how to do this, please see "Displaying Hidden or System Files" on page 62.

Chapter 3 – Client/Server Configuration

This chapter contains information on the following:

- Getting Started
- User Configuration
- Adding Devices
- Configuring Devices using the Web Interface
- Deleting Devices
- Configuring Video Sources
- Configuring Triggers
- Configuring Pan-Tilt-Zoom Capabilities
- Configuring Audio
- Configuring Sequences

VSolP Lite contains several configurable aspects, including collections of IP cameras and Networked DVRs.

Getting Started

We recommend that you take the following steps when configuring VSolP Lite:

- 1 Start VSolP Lite. To do this, select Programs>VSolPSuite Lite from the Start menu.

Note: If the application does not start, this may be because another instance of the application has been detected. If the other instance is running normally, it is brought to the front. If the other instance is in the process of shutting down, it is terminated immediately and the new instance is started.

- 2 Log in as the default administrative user. The default user is *admin*, password *admin*.
- 3 Add devices to the system.
- 4 Configure alarm triggers.

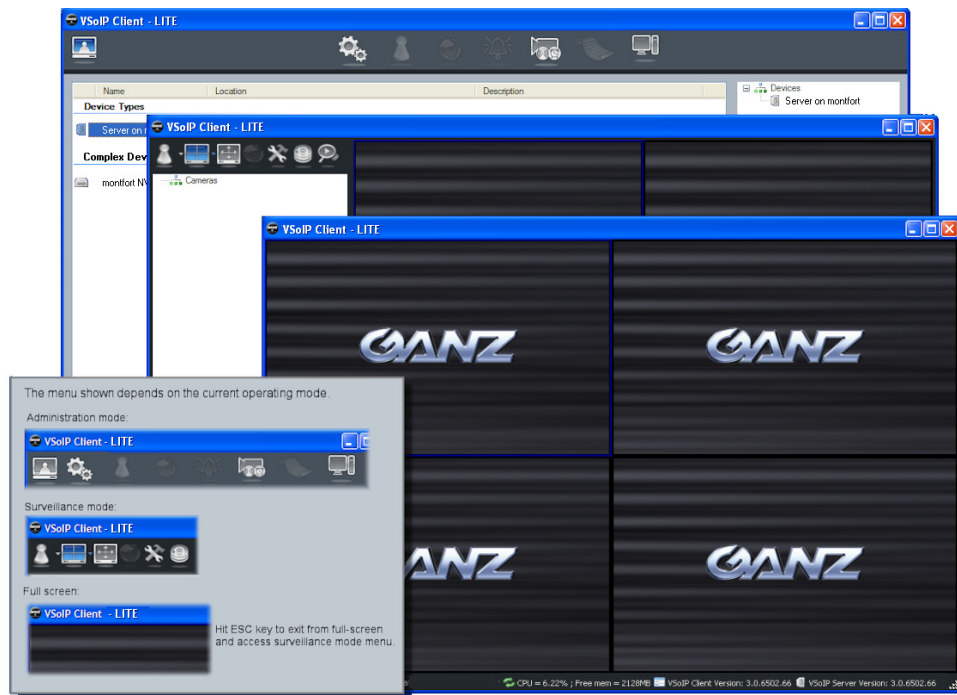


Figure 4 Accessing VSoIP Lite's main menu

User Configuration

VSoIP Lite is preconfigured with three users - Administrator, Manager and Operator.



- **Administrator** — has access to all functionality. To log in as administrator, use the user name *admin* and password *admin*.
- **Manager** — has access to all functionality, with the exception of adding, editing or deleting devices and disabling recording schedules. To log in as the manager user, use the user name *manager* and password *manager*.
- **Operator** — can view live and recorded video. To log in as the operator user, use the user name *operator* and password *operator*.

Note: For security reasons, these default user names and passwords should be changed the first time they are used.

Changing User Passwords

Changing User Passwords

Any logged-in user can change their password. To do this:

- 1 Select  in the top left corner, then .
- 2 Enter the current password for your user account, then enter a new one and confirm it.
- 3 Your password is changed. Please keep a note of your password in a safe place.

Device Configuration

A device can be one of the following:

- An IP camera.
- An IP encoder.
- A Networked DVR.

Some devices, such as a Networked DVR or an IP encoder can have several analogue camera inputs. In addition, certain devices have multiple encoders for each analogue camera input.

This means that a single device such as an IP camera could generate several video sources, one for each encoder built in to the camera.

Some devices support trigger inputs. These are sources that signal that some event has occurred. For some devices this represents a simple electrical voltage being applied to a single input pin.

IP cameras, Networked DVRs and encoders can optionally support Pan-Tilt-Zoom (PTZ) devices. A PTZ device allows the camera's field-of-view to be altered using the pan-tilt-zoom controls in VSoIP Lite.

Note: The surveillance system is preconfigured with a number of types of Ganz IP cameras, Networked DVRs, pan-tilt-zoom control units and protocols.

Adding Devices

There are two methods of adding a device to the server. Many devices can be added using autodiscovery. (This depends on which discovery protocols they support and whether the network allows discovery information to be transmitted.) Those that cannot be added in this way must be added manually.

Note: If using autodiscovery, please note that multicast-based discovery broadcasts used to discover devices or servers will not work correctly when the network connection used has Internet Protocol Version 6 (TCP/IPV6) enabled. Ensure Internet Protocol version 4 is enabled and then disable TCP/IPV6, as shown in Figure 5. On computers where only one Internet Protocol (TCP/IP) is listed then typically this is version 4 and no further modification is required.

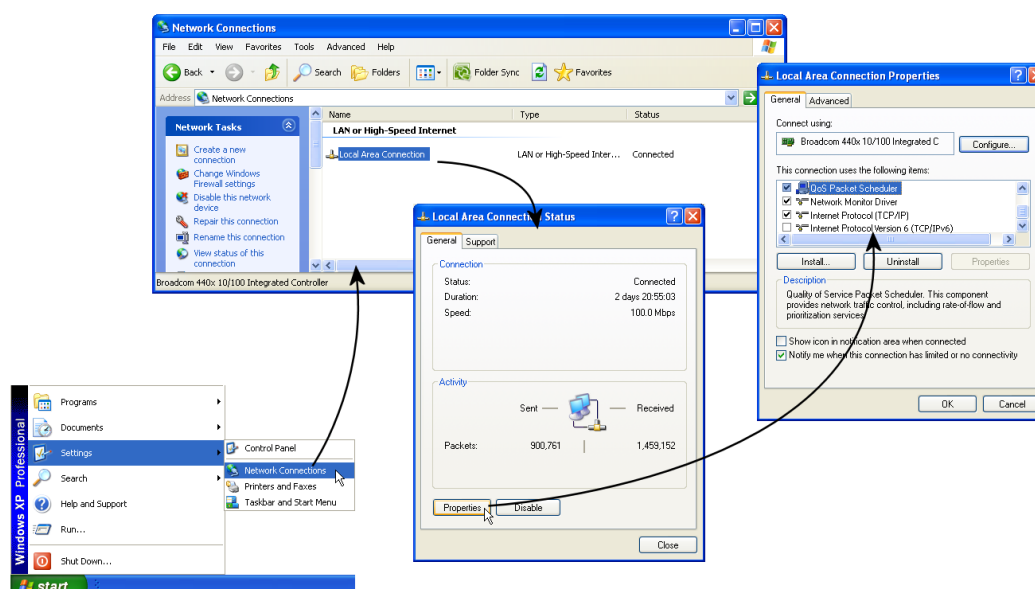


Figure 5 Disabling TCP/IPV6

Adding a Device Using Autodiscovery

VSoIP Lite can perform a scan of the network and list the devices which it finds. To add a device using autodiscovery, follow the steps shown in Figure 6:

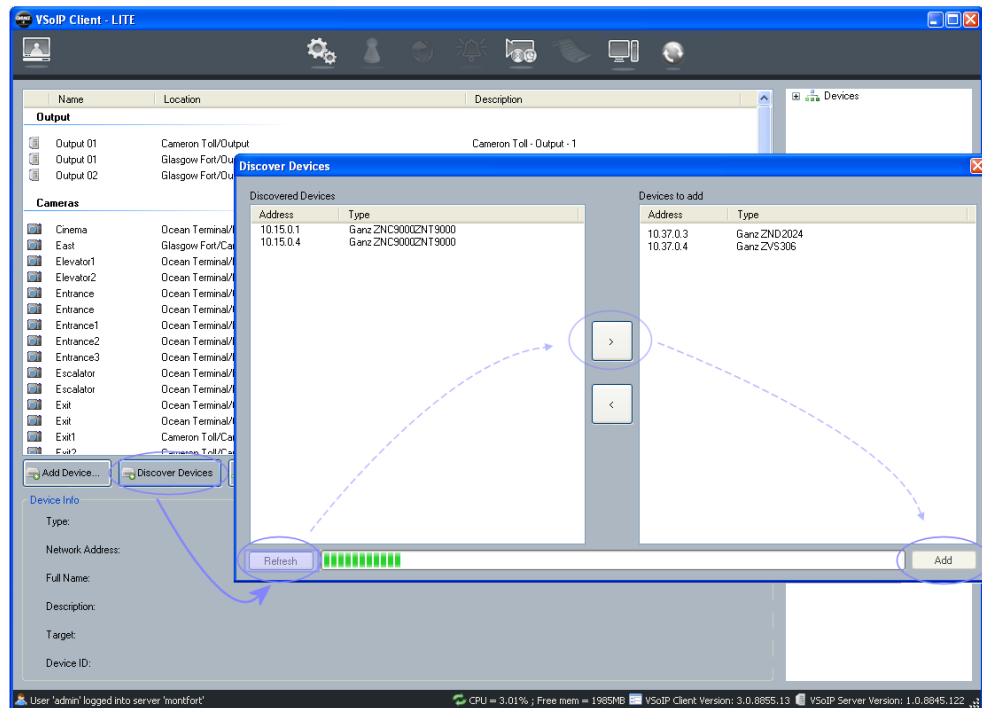


Figure 6 Adding a device using autodiscovery

- 1 A list of all devices discovered on the network is shown. Select the device(s) you require and click the arrow to add them to the site, then click Add, as shown in Figure 6.
- 2 You are prompted to add or amend details for each device in turn that you have added.

Caution: Please ensure that the correct codec and transport options are selected for each device (where available), as the default option may not be applicable to all device types.

Adding a Device Manually

If a device has not been discovered by the network scan, you must add it manually as follows:

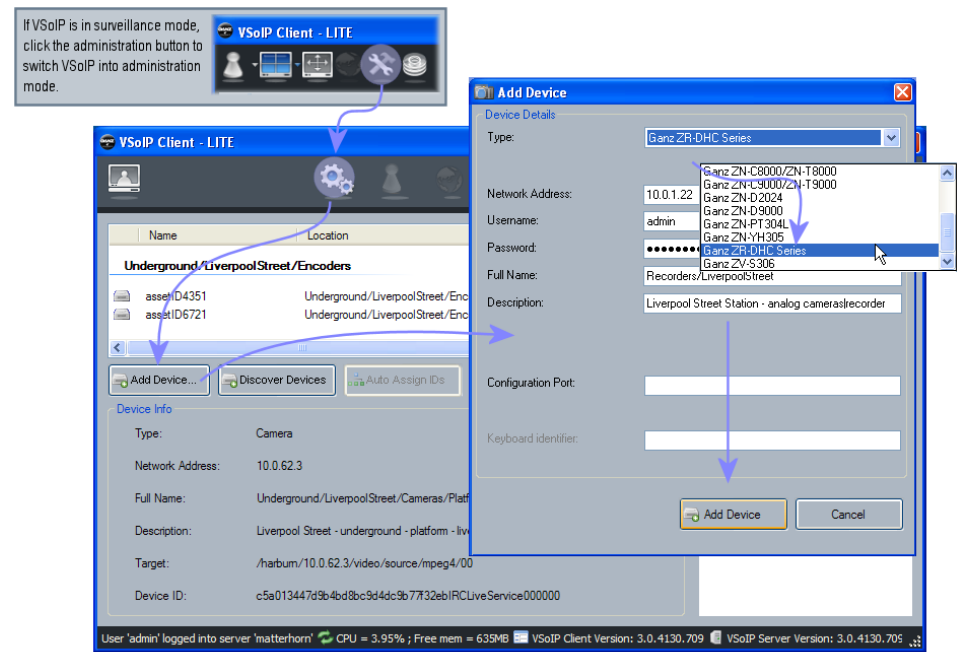


Figure 7 Adding a device

Add the required device as indicated in Figure 7.

Note: Only alphanumeric characters, spaces, forward slash (/) and underscore (_) can be used for the device name. Note that you must allocate a username and password to the device. These must contain only alphanumeric characters.

Note: If you are adding a device which needs to use a particular port number to support video streaming, eg RTSP, add it after the IP address, in the format 192.168.1.2:554. If you are adding a ZV-S306 camera, please see Appendix C, "Specific Device Considerations" for more information.

Caution: When adding an IP camera, encoder or Networked DVR, ensure that the device has been configured so that the device type selected in VSoIP Lite matches the operational parameters of that device.

For example, an IP camera may offer MJPEG, MPEG4 and H.264 as video stream encoding types. If the encoding type has been set to MPEG4 using the camera manufacturer's configuration method, MPEG4 must also be selected when adding the camera to VSoIP Lite. This is done by selecting the correct device type (or sub type) — so for this example, a device type is chosen that matches manufacturer name, device family and that lists MPEG4 as the encoding type.

For example, for the ZN-S1000VE device type, you would choose the MPEG4 option:

ZN-S1000VE	H264
ZN-S1000VE	MPEG2
ZN-S1000VE	MPEG4

Using Location Text

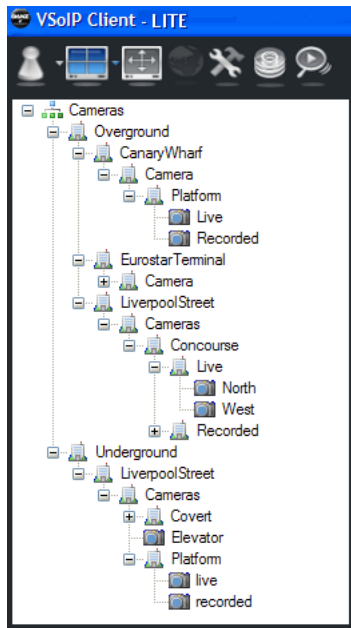


Figure 8 Device hierarchy example

Location text is used to logically group devices. An example of the location text can be seen by looking at the presentation of the device hierarchy or "site". When constructing a location string each level of the hierarchy is defined by the use of the forward slash character, e.g. '/'.

If the location string is left blank then the name of the device is the sole label for the device and is shown at the top level of the hierarchy. A location string entered without slashes adds the device one level down in the hierarchy with a top level entry labelled by the location string. A location string containing two labels separated with a single slash adds the device two levels down the hierarchy, with the text before the slash labelling the device at the top level, the text after the slash labelling the device at the second level and then finally the name of the device labelling the third level.

By naming different devices with common top, second, third, etc location text labels, a number of devices can share some or all of the same location.

Some location text examples as shown in Figure 8:

- Overground (shared with Canary Wharf, EurostarTerminal and LiverpoolStreet)
- Underground (shared with LiverpoolStreet)

Location Text Example

Assume you have a series of video sources with views of different sections of a warehouse.

- Three IP cameras viewing bay one in goods-inward: Cam1, Cam2, and Cam3.
- Two IP cameras in bay two of goods-inward: Cam1 and Cam2.
- Three IP cameras in goods-outward: Cam1, Cam2 and Cam3.

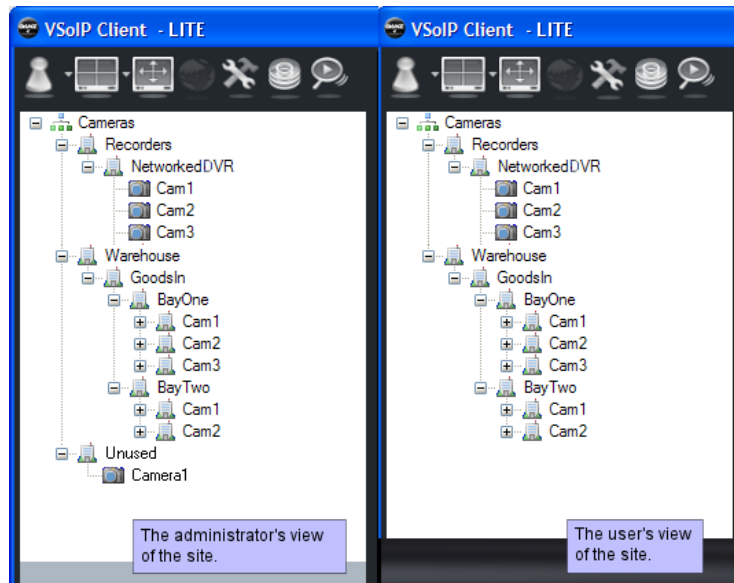


Figure 9 Warehouse site location text example

- 1 Add three IP camera devices with names Cam1, Cam2 and Cam3 and use the same location text: Warehouse/GoodsIn/BayOne.
- 2 Next add two more IP camera devices with names Cam1 and Cam2 and use the same location text for both: Warehouse/GoodsIn/BayTwo.
- 3 Add a Networked DVR device named NetworkedDVR with location text Recorders.
- 4 Next name inputs 1, 2 and 3 of the DVR Cam1, Cam2 and Cam3 respectively.

Using the name and location text as described above will result in a site as shown in Figure 9.

Configuring Devices using the Web Interface

VSolP Lite allows you to alter a device's configuration once you have added it to the server.

When you add a device to your network, VSolP Lite receives a configuration URL from the device which allows it to access the device's web-based configuration. If your network has a firewall, you may first need to add a specific port number to this configuration URL to ensure that VSolP Lite can access the device's configuration page. Figure 10 shows how to do this:

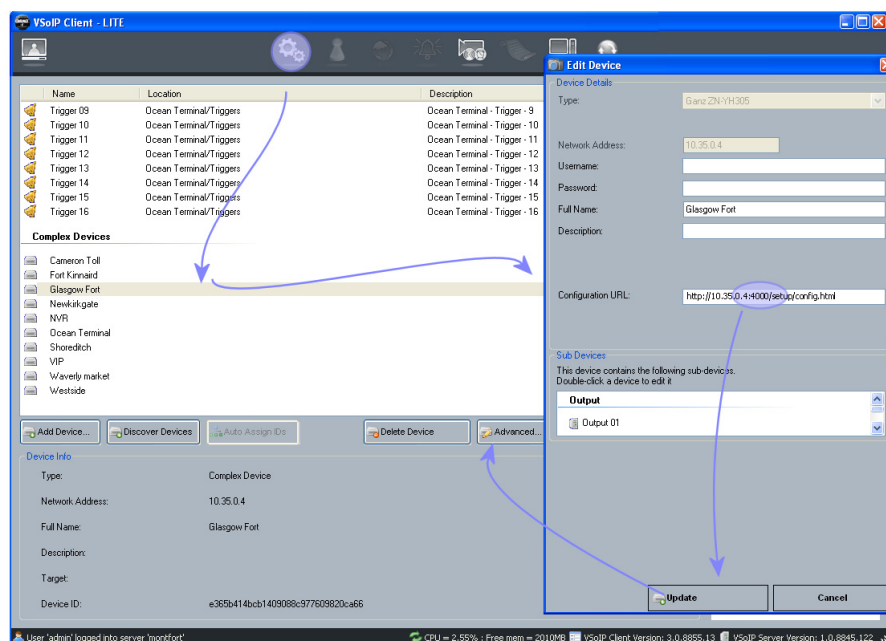


Figure 10 Ensuring device configuration access through a firewall

Once you have added this port number, if required, click Advanced to access the device's web configuration pages.

Note: To configure a device with multiple inputs, ensure that you select the encoder name from the list. For example, in Figure 11, you would select Glasgow Fort.

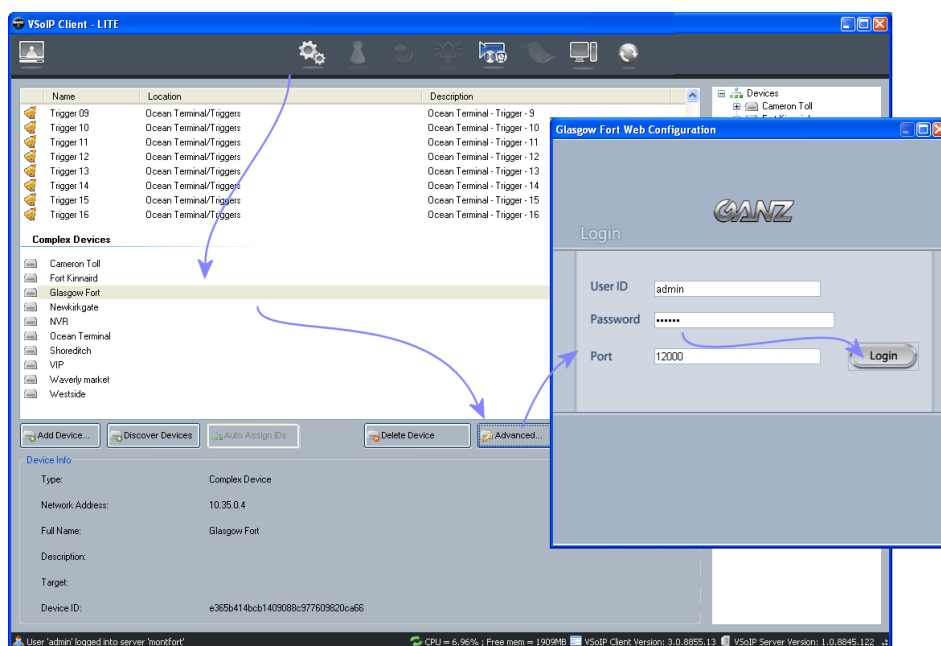


Figure 11 Configuring devices from VSolP Lite using web page

Deleting Devices

Caution: Before deleting a device, please ensure that no recordings jobs are associated with it. If this is the case, please delete these recording jobs before continuing.

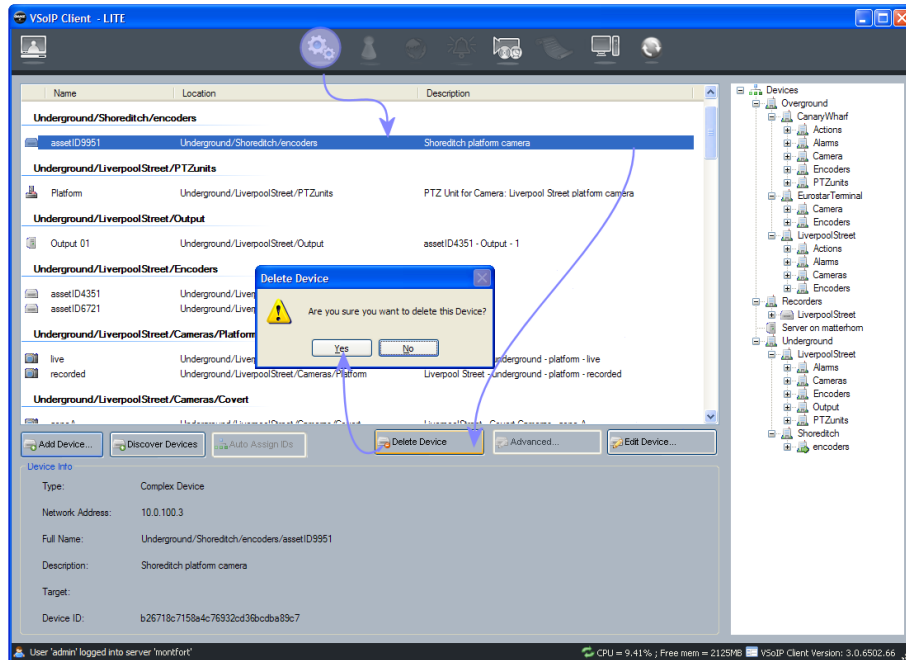


Figure 12 Deleting a device

Note: When deleting a device such as an IP encoder, all associated sub-devices related to that device are also deleted, e.g. PTZ units, etc.

Configuring Video Sources

An IP camera or Networked DVR supports one or more video sources. Each video source has a default name. When a device is initially added to the system, the various video sources are named automatically and grouped into a sub-hierarchy under the device.

The automatically assigned name and location text can be changed, allowing you to group the video sources logically.

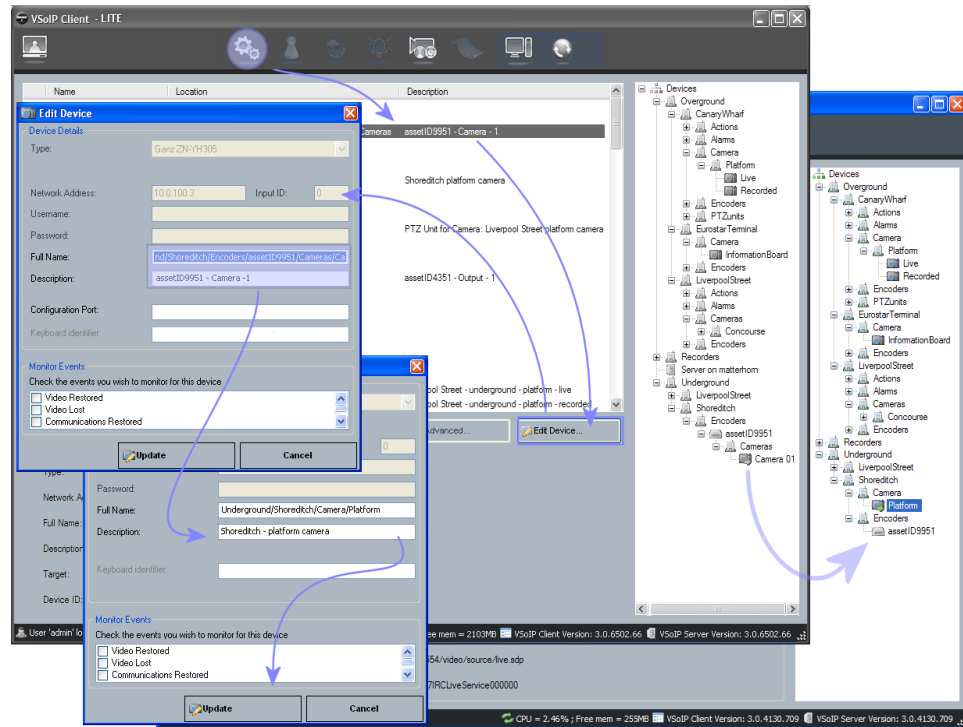


Figure 13 Renaming/setting location for video source

Note: All Networked DVRs can be grouped together in their own logical group of recording devices using the location text. The location text for the various video sources of IP cameras and Networked DVRs can then be renamed and modified to allow the physical layout of the surveillance site to be readily understood from the site/device hierarchy.

Configuring Triggers

A trigger is the source of an alarm, such as an alarm contact on an IP camera or a Networked DVR.

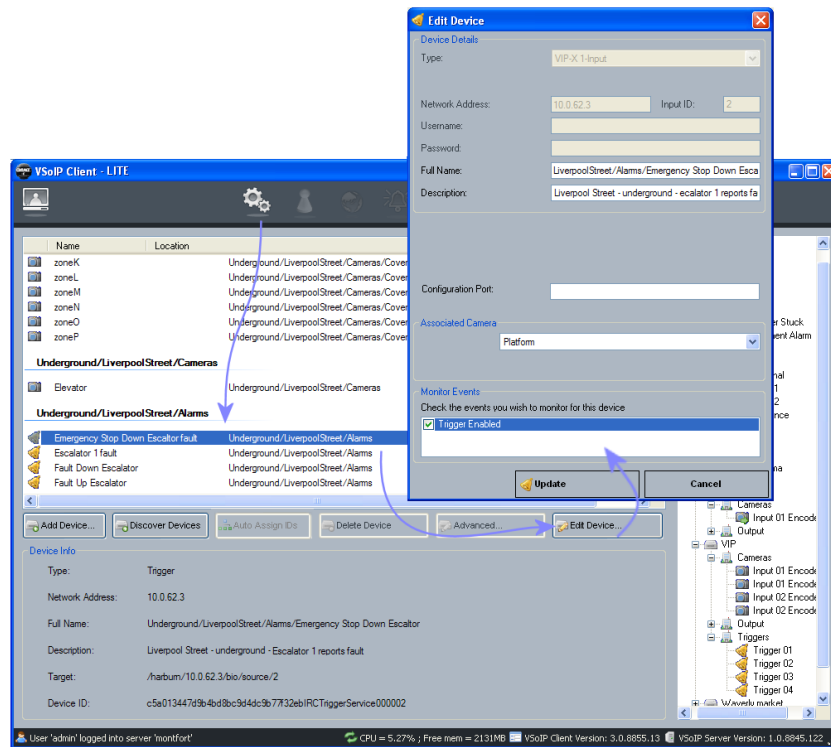


Figure 14 Activating and naming triggers

To activate a trigger:

- 1 Select the alarm you want to edit from the list and click Edit Device.
- 2 Select the camera associated with this alarm. This allows operators interacting with the alarm to easily see a related video feed.
- 3 Check Trigger Enabled. This allows VSoIP Lite to receive alarms.
- 4 Click Update.

Note: There may be a lag time between connection loss of a given device and the raising of an alarm indicating the connection loss. This lag can be anything between 30 and 90 seconds, depending on device and server activity.

Note: Triggers can either be actively monitored or not. When updating a trigger make sure that you have enabled monitoring of events for that trigger.

Use the location text to logically group triggers into groups that make sense for the physical site being monitored.

You cannot delete triggers. If one or more triggers available from a device are not required, then disable monitoring of each trigger event. You can collect unused triggers together under a logical group of unused triggers, keeping them separated from the triggers in use.

Configuring Pan-Tilt-Zoom Capabilities

IP cameras and Networked DVRs can provide connections that enable one or more pan-tilt-zoom control units to be attached. In some cases the IP camera includes a built-in pan-tilt-zoom controller.

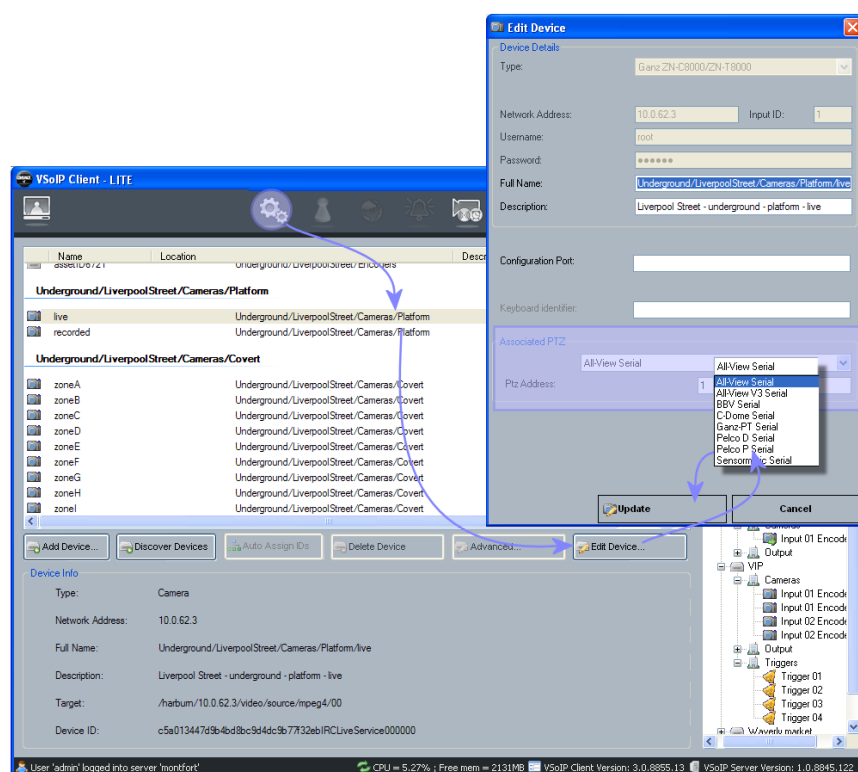


Figure 15 Enabling PTZ capability for a video source

Caution: When you have finished making changes to a device's configuration, you should restart/re-establish any open connections to the device to ensure that the changes take effect.

Some cameras, typically those attached to video encoders, might be connected to a PTZ controller unit. This is usually done using the serial port of the video encoder. E.g. ZN-T9000 connected to a C-ALLVIEW.

A typical arrangement with encoders is to use several analogue inputs alongside several PTZ units. The CCTV installer will use different PTZ addresses when sharing a common serial port.

Under this arrangement, find out the appropriate PTZ address for the camera and PTZ unit pairing and set the appropriate PTZ address when associating a PTZ with an analogue camera.

Configuring Audio

VSoIP Lite supports two-way audio to allow communication with devices which support audio. As shown in Figure 16, audio can either be one way, or both ways between source and destination devices.

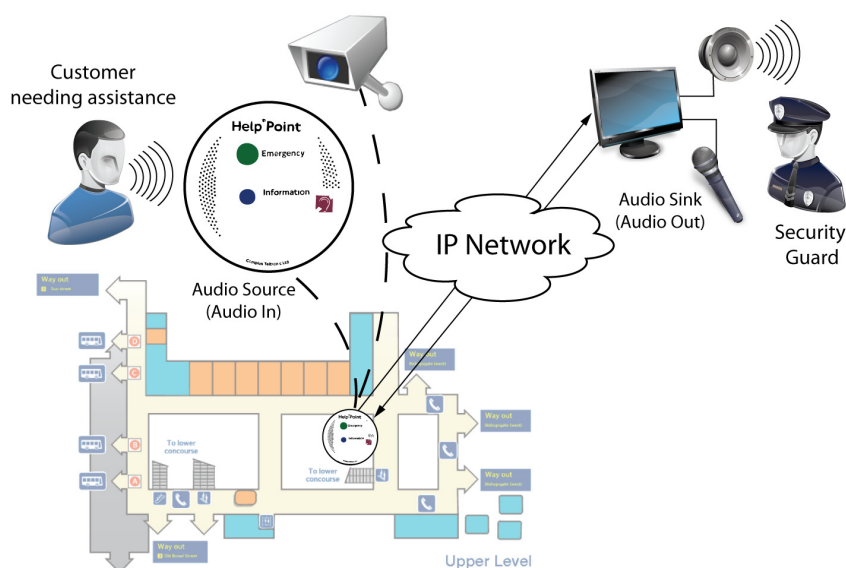


Figure 16 Example of two way audio communication

To configure audio settings:

- 1 Add an audio-compatible device (see “Adding Devices” on page 19 for information on how to add a device).
- 2 Select the device you want to configure and click Edit Device.

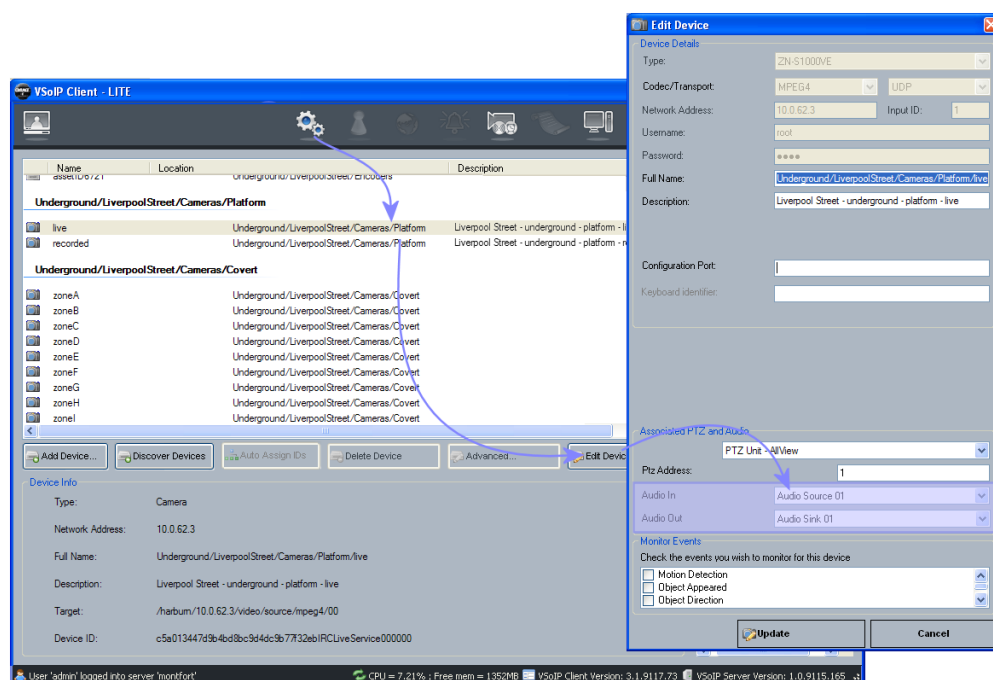


Figure 17 Configuring audio on a device

- 3 Select the required devices for Audio In and Audio Out respectively (see Figure 17).
- 4 Click Update to save the settings.

After specifying the audio devices, you can specify how the audio functionality should be controlled within VSoIP Lite. This is configured using the System Settings dialog.

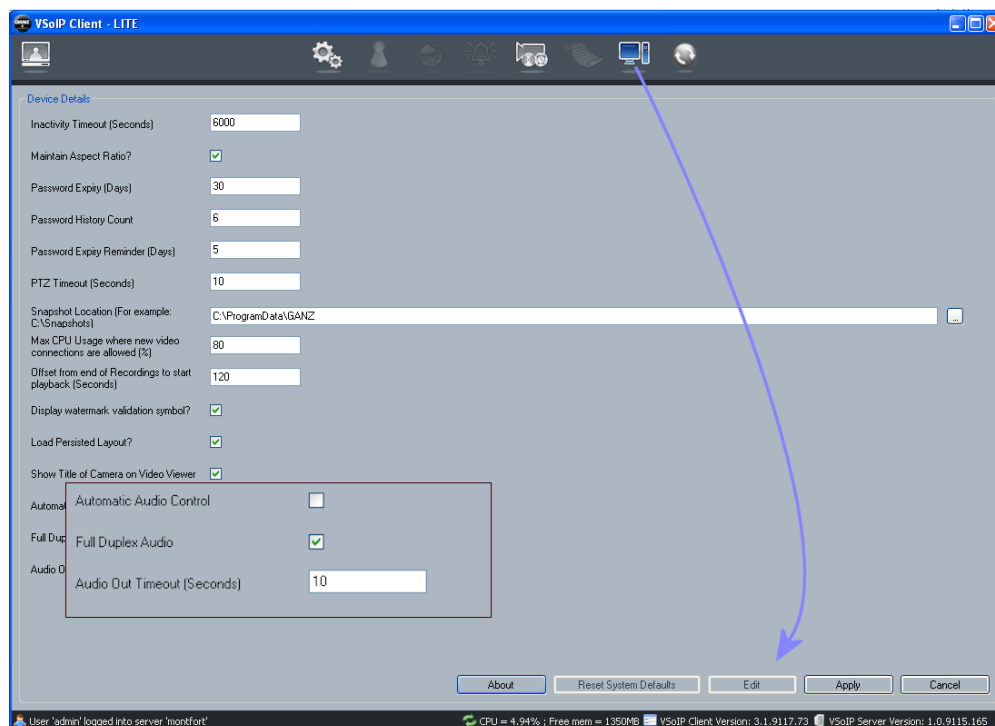



Figure 18 Audio system settings



Caution: When you have finished making changes to a device's configuration, you should restart/re-establish any open connections to the device to ensure that the changes take effect.

Communicating Using Audio


When audio is available for a camera displayed in a video pane, the  symbol is shown in the corner of the pane.

Listening to Audio from a Camera

Audio can be used in two modes:

- **Automatic**
Select Enabled to use audio in automatic mode. This enables audio in all panes displaying cameras which support audio. Audio is played from the pane which is selected (this may be by clicking on a camera on a map, or simply by clicking a pane which is already displaying video). Changing the selected pane turns off the audio feed in the initial pane, and starts it in the second pane.
- **Manual**
Deselect Enabled to use audio in manual mode. You may want to disable Automatic Audio if you frequently switch between panes for other purposes, for example, controlling PTZ cameras. When disabled, you must first select the pane displaying the camera whose audio you want to hear, then click . To listen to audio from a different camera, select the pane playing the second camera, then click  again.

Using a Microphone

To use your microphone to communicate with someone on screen, click the appropriate pane and then click . The microphone then remains active until it times out. (See “Audio Out Timeout”, below.)

Preventing Feedback

If you are experiencing feedback when interacting with cameras on screen, disable Full Duplex Audio (Figure 18). This sets the audio mode to Half-Duplex — allowing communication in both directions, but in only one direction at a time.

Audio Out Timeout

This value specifies how long a microphone can be used for before the connection times out.

Configuring Sequences

A sequence is a group of cameras which are displayed sequentially within a single video pane, either on a client or on a Video-wall, each for a configurable length of time. Any number of cameras can be added to a sequence. To create a sequence:

- 1 Select Sequences in the Administration pane, as shown in Figure 19.

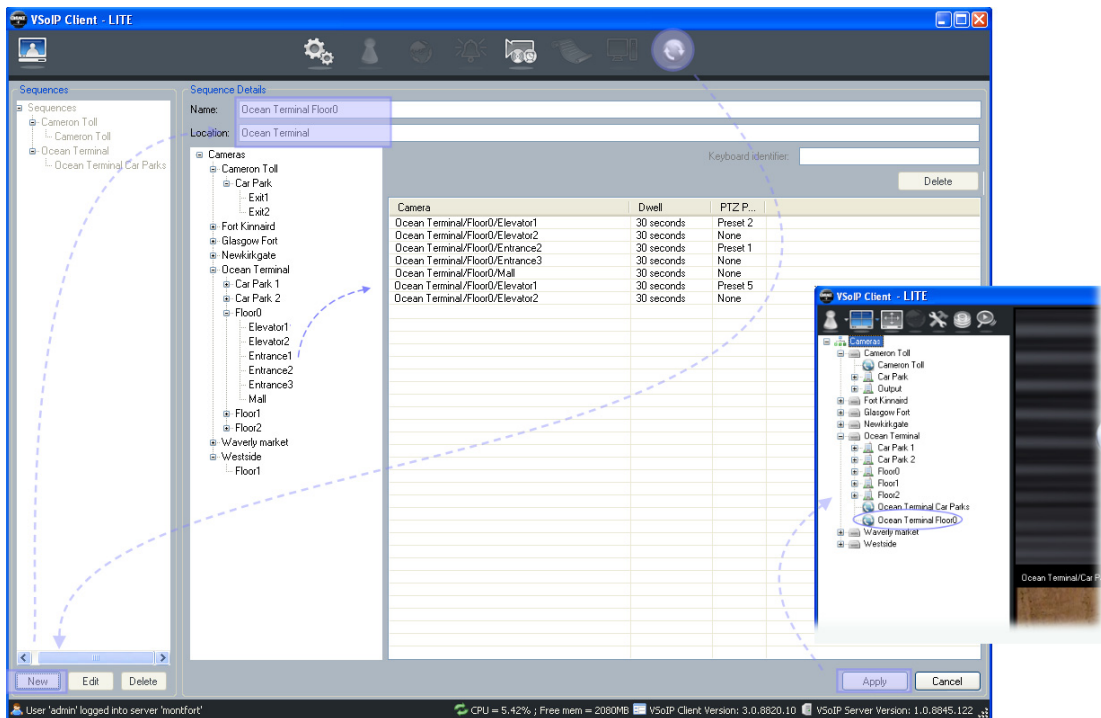


Figure 19 Creating a sequence

- 2 Select New.
 - 3 Enter a name and location for the sequence.
 - 4 Select a camera in the sequence tree and drag and drop it into the sequence.
- Note:** Individual cameras can be added more than once to a sequence.
- 5 Alter the dwell time if required to change the length of time footage from each camera remains on screen.
 - 6 Select a PTZ preset, if required.
 - 7 Add all required cameras, then click Apply.

Note: To edit or delete an existing sequence, select the required sequence in the list and click Edit or Delete, as required.

Chapter 4 – Using VSoIP Lite to Monitor your Site

This chapter contains information on the following:

- Working with Live Video and PTZ
- Working with Alarms

Working with Live Video and PTZ

VSoIP Lite allows CCTV operators to view live video from up to 36 IP cameras, cameras attached to networked DVRs and cameras attached to IP encoders. It also allows the operator to move pan-tilt-zoom (PTZ) cameras, to zoom in closer to the scene displayed, and to take a snapshot of a particular moment. The video panes making up the operator's viewing area can be laid out in various ways as suits the operator's needs and the capabilities of the display hardware.

Live Video Controls

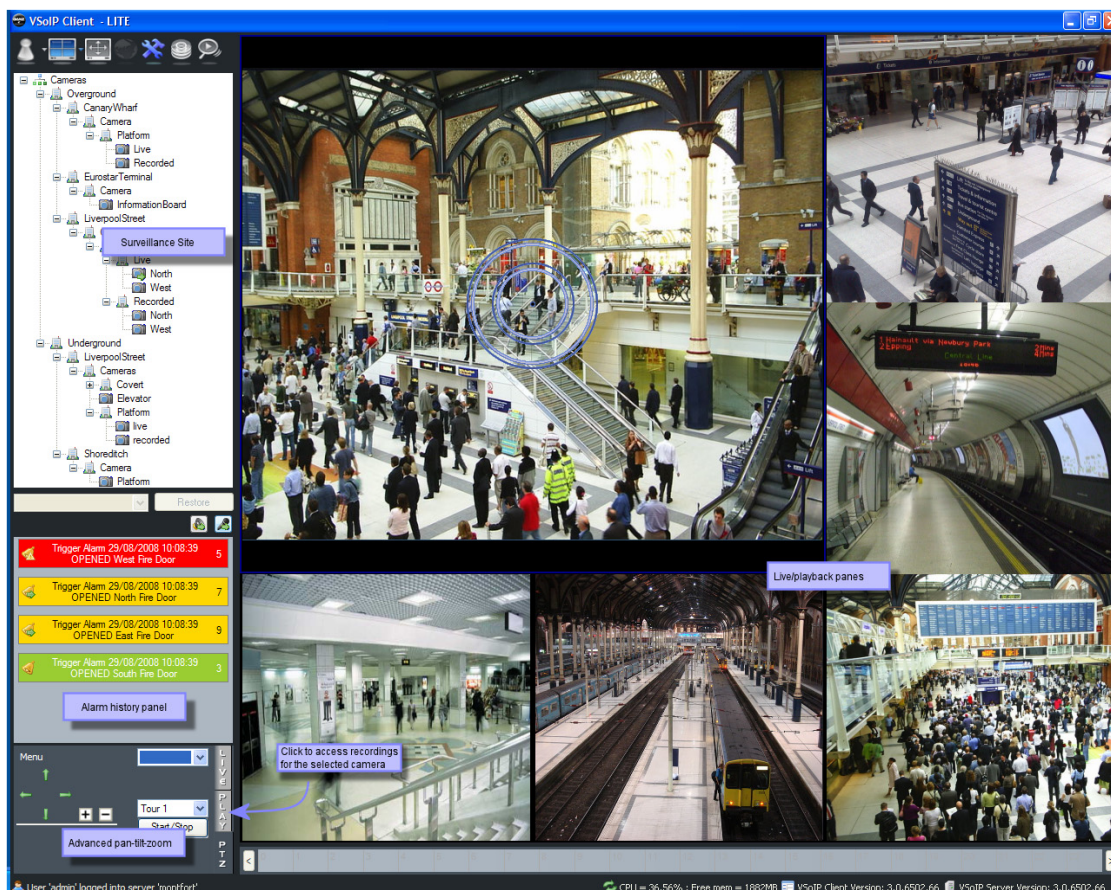


Figure 20 Main live viewing controls

Accessing other features

The main menu can be used to switch VSoIP Lite into various surveillance modes.

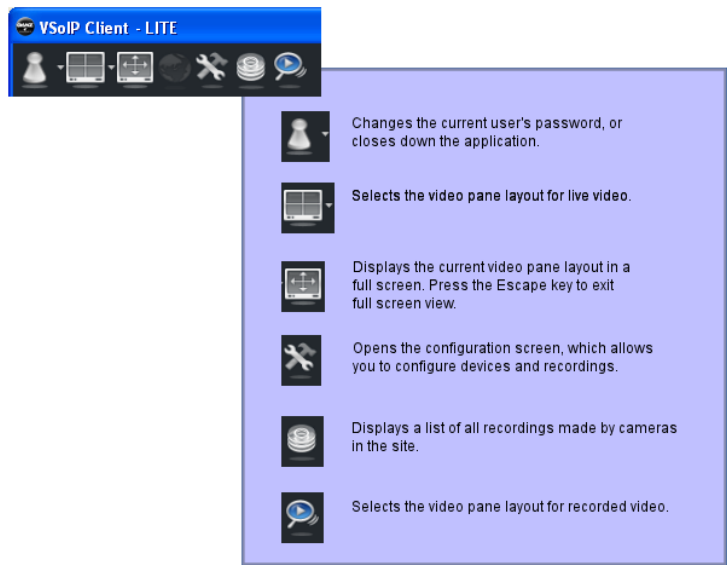



Figure 21 Location of main menu

Specifying Video Pane Layout

To specify a video pane layout, click  and select the required layout from the drop down menu.

Double-click any pane to maximise it. Double-click again to restore it to its original size.

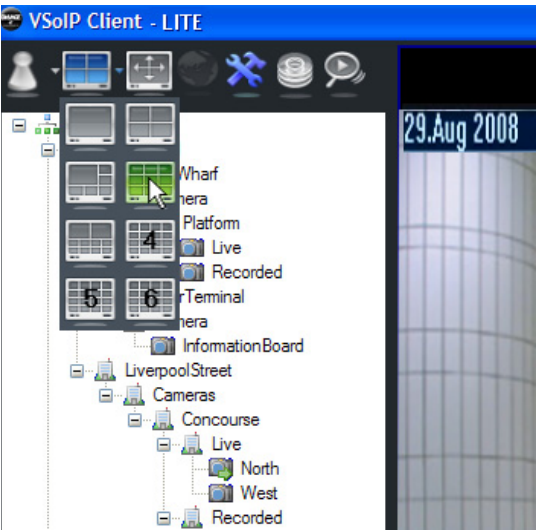


Figure 22 Selecting a video pane layout

Starting and Stopping Live Video

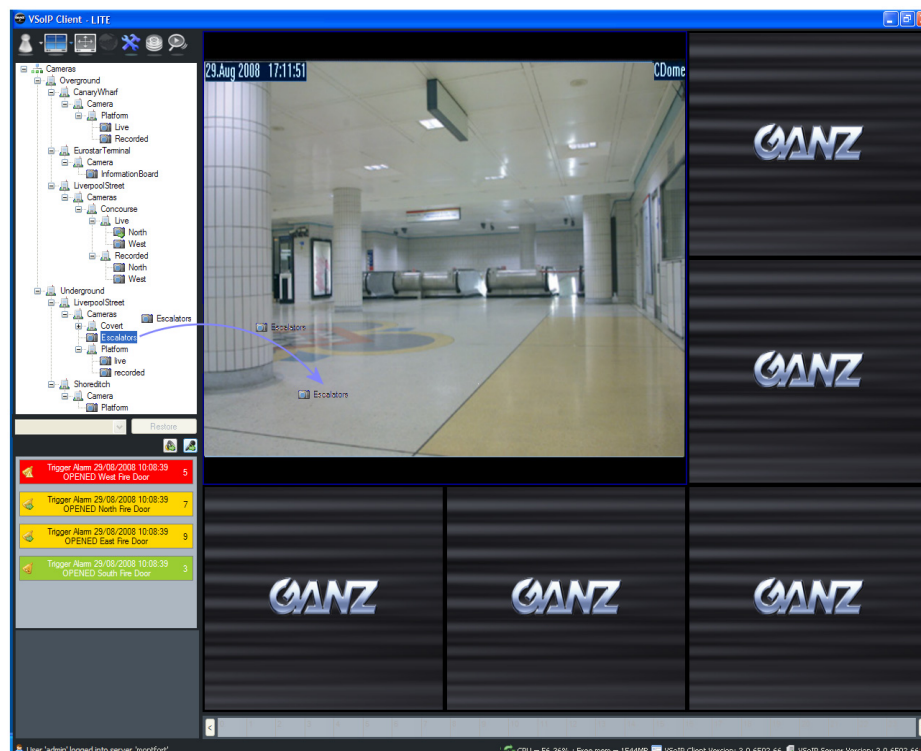


Figure 23 Starting video using mouse drag-drop

To start video in a video pane, either on the main monitor, or on an additional monitor (if you have a multi-head setup), select the camera in the tree and drag and drop it onto the required video pane. To activate relevant functions for the camera in that pane (for example, PTZ functionality), click once in the video pane. Alternatively, select the pane before dragging and dropping a camera into it.

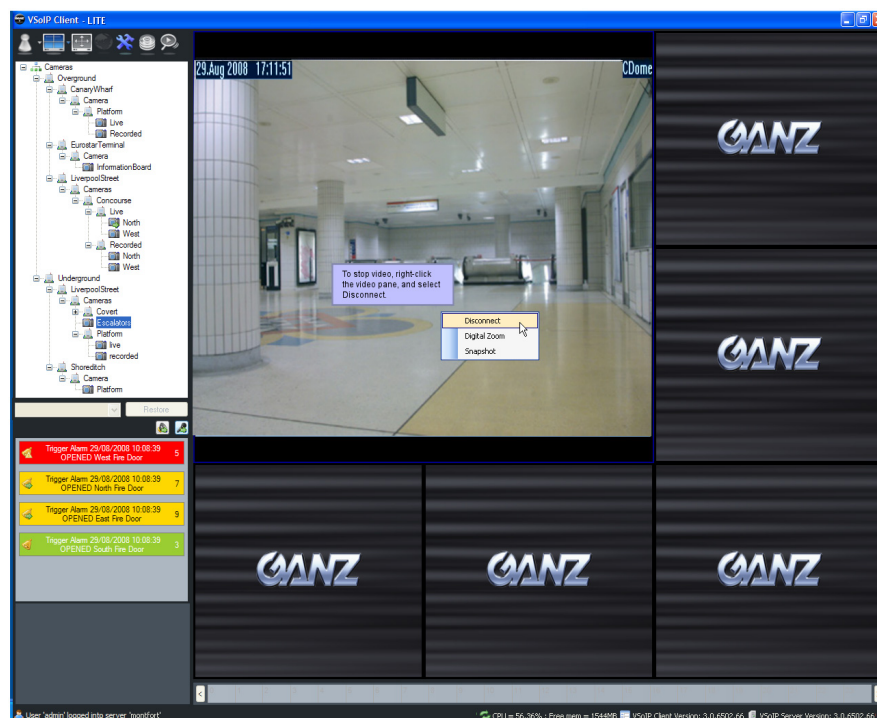


Figure 24 Stopping video

Using Digital Zoom

VSolP Lite allows you to zoom in on and move around live video footage.



Figure 25 Zooming into live video

Right-click the video pane and select Digital Zoom. Click the part of the pane that you want to see in more detail, then use the mouse scroll button to zoom in and out as required. While zoomed in, click away from the centre of the image and drag the mouse to pan the video.

Taking a Snapshot of Live Video

VSolP Lite allows you to capture snapshots of live video playing in a video pane. These are saved to \\Desktop\\VSolP Image Clips\\FromLiveDevices, as .jpeg images. To change this location, see “Default Settings” on page 58.

To take a snapshot, right-click in the pane displaying the video at the point you want to capture, and select Snapshot.

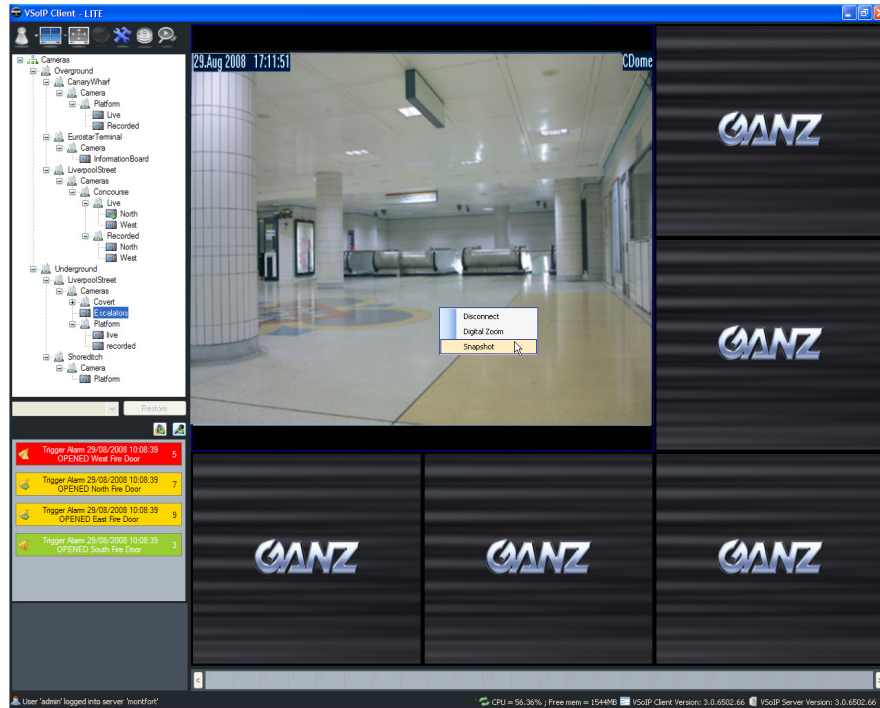


Figure 26 Taking a snapshot of live video

Control of Pan-Tilt-Zoom

Activation/Deactivation

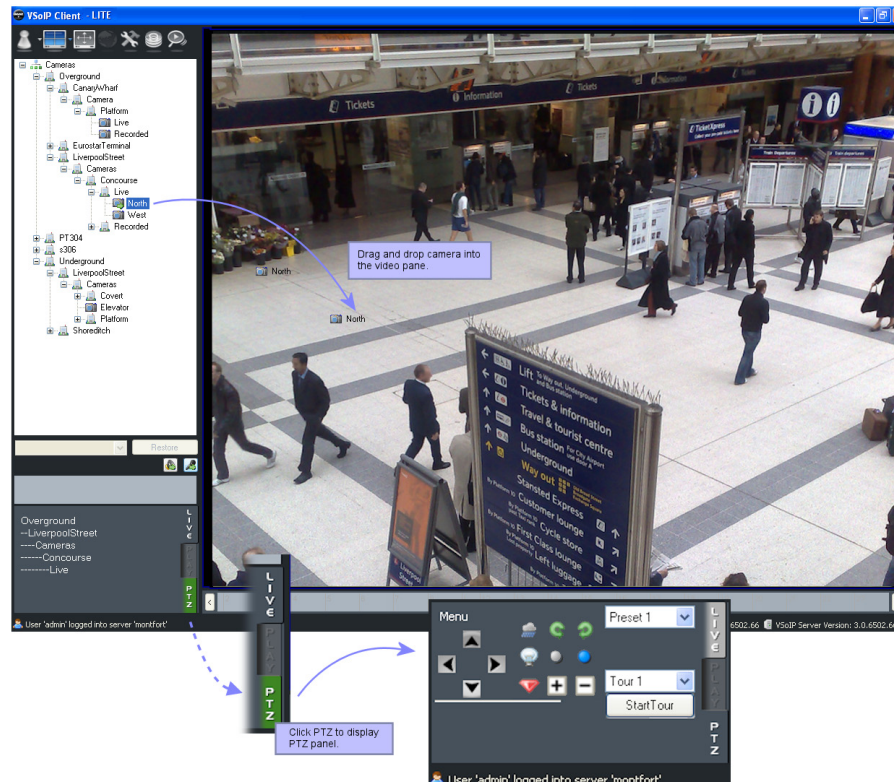


Figure 27 Activating/deactivating PTZ support

Moving and Zooming

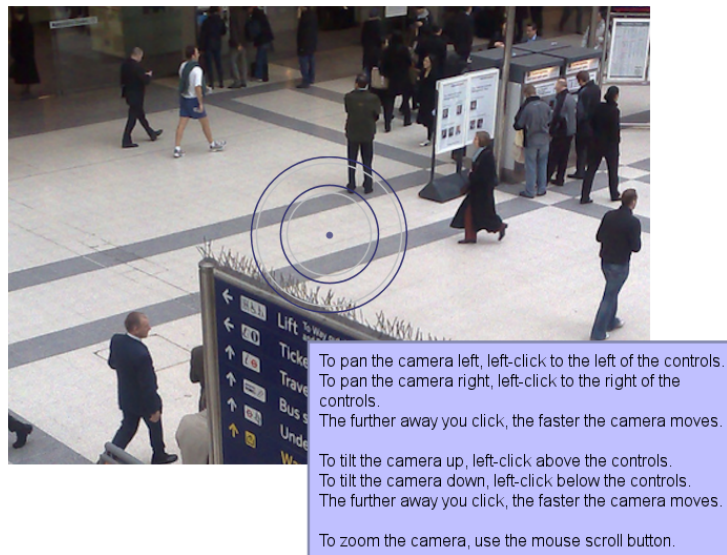


Figure 28 Panning, tilting and zooming

Extra features

Some PTZ cameras and protocols provide access to extra functionality, which allows you to carry out extra commands, such as using presets or tours. These are detailed below.

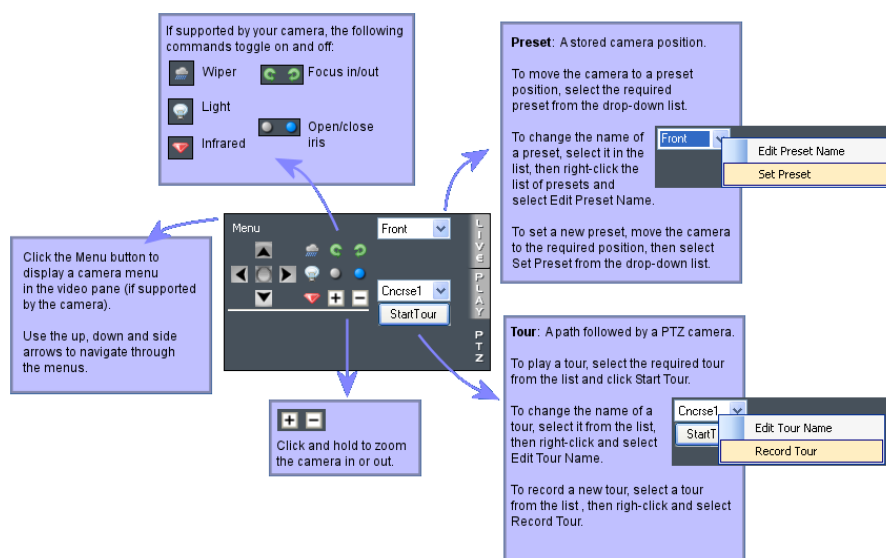


Figure 29 Additional PTZ unit features support

Note: PTZs vary in functionality, so access to features depends on the chosen PTZ unit's capability.

Viewing Sequences

Sequences display a loop of continuous video from different cameras within a video pane. For information on how to set up sequences, see "Configuring Sequences" on page 31.

To view a sequence:

- 1 Navigate to the sequence you want to view in the tree.
- 2 Drag and drop the sequence into a video pane (Figure 30).



Figure 30 Viewing a sequence

Caution: Before setting up or using a sequence, you should first calculate the combined bandwidth of all participants in the sequence. For example, you might have a single 2Mbps capped H264 stream from a UDP Tech IPE1100 camera, a 768 kbps capped MPEG4 stream from a Bosch VIPx and a 2.3Mbps MJPEG stream from an Arecont AV1300 camera. The bandwidth attributable to the sequencing pane in the client would be $2048 + 768 + 2356 = 5172\text{Kbps}$ or 5Mbps.

To stop a sequence, right-click the pane in which the sequence is playing and select Disconnect.

Working with Alarms

The alarm display presents unacknowledged, acknowledged and closed alarms.

Note: To enable VSoIP Lite to display an alarm for a particular alarm source, e.g. contacts on a Networked DVR, the alarm type for the device associated with the alarm source must have been enabled. For details, see “Configuring Triggers” on page 27.

Overview of Alarm Display

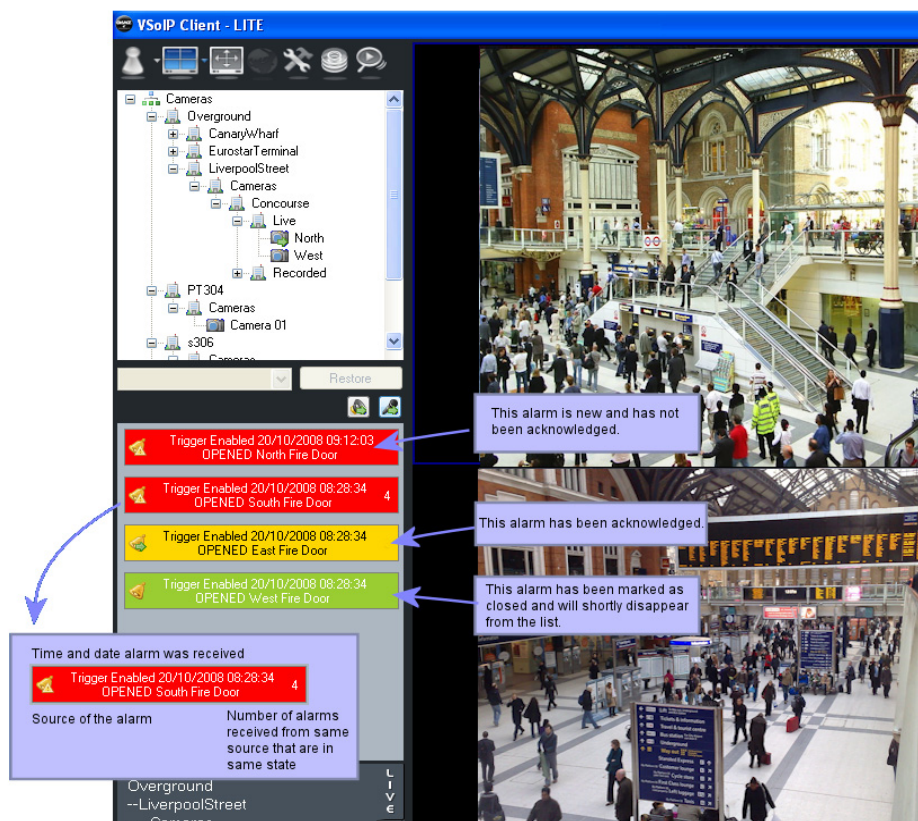


Figure 31 Overview of alarm display

Viewing Properties of an Alarm

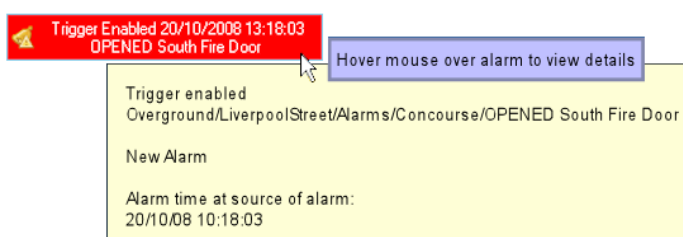


Figure 32 Alarm properties

Note: As shown in Figure 32, the time shown in the tool tip may vary from the time displayed for the alarm. Where possible, the tool tip displays the time the alarm was generated at its source, whereas the alarm entry displays the local time.

Note: There may be a lag time between connection loss of a given device and the raising of an alarm indicating the connection loss. This lag can be anything between 30 and 90 seconds, depending on device and server activity.

Acknowledging an Alarm

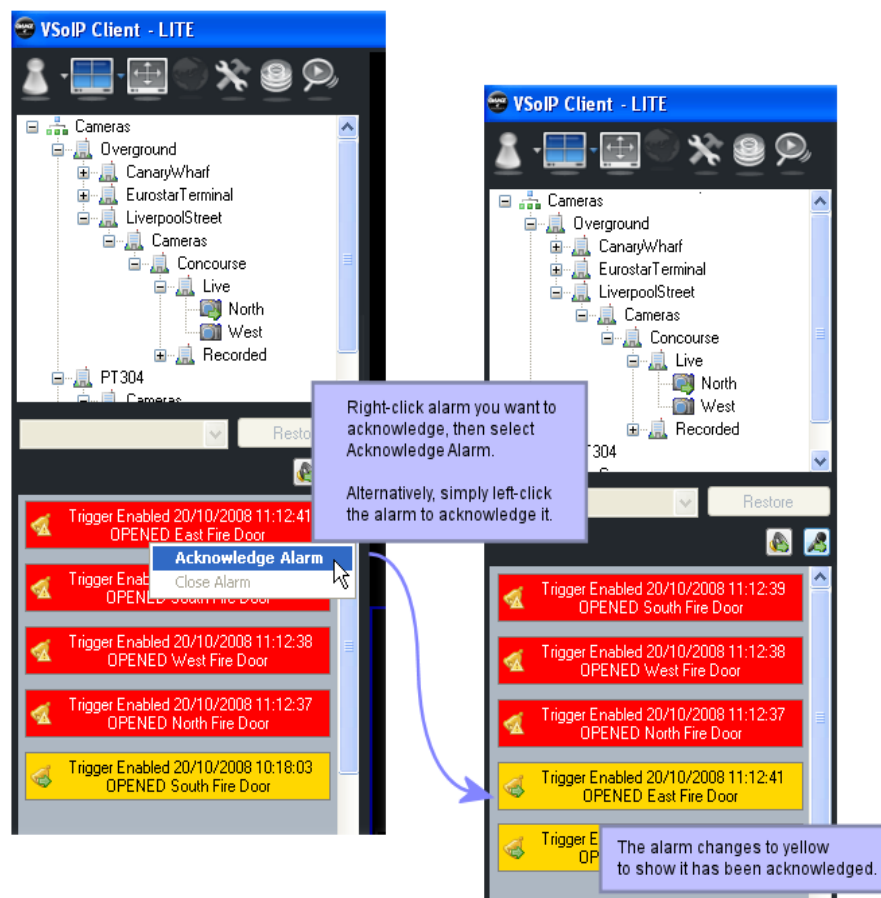


Figure 33 Acknowledging an alarm

Closing an Alarm

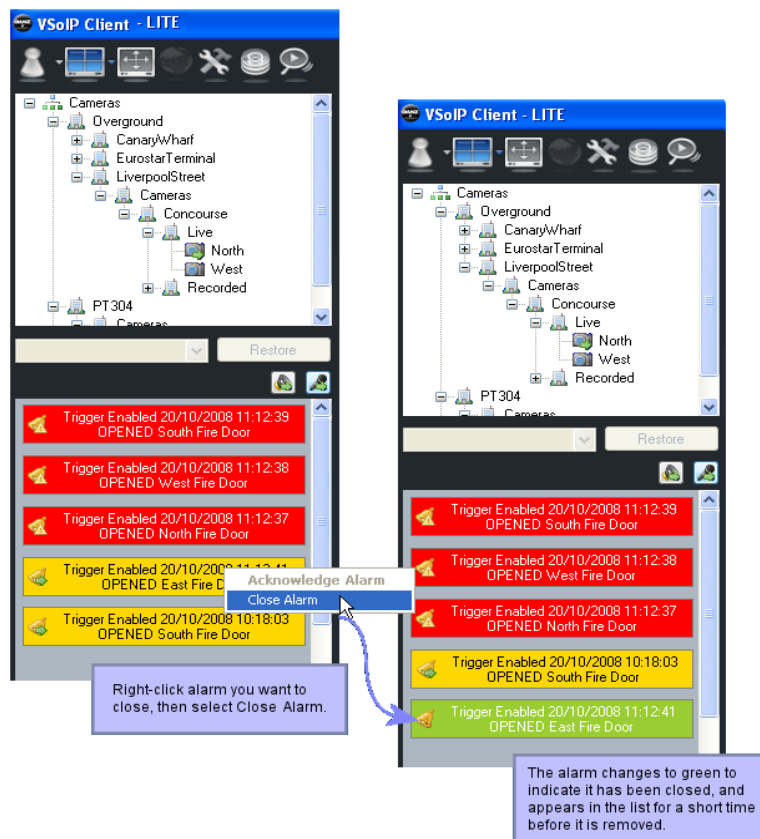


Figure 34 Closing an alarm

The Audit Trail

The audit trail provides a list of events that have occurred since VSoIP Lite was installed. Some examples of event information are:

- Alarms (acknowledgement, closed).
- Devices (added, updated, deleted, disconnected etc.).
- Recording (disk space low or critical).

This list is not comprehensive – many other types of event are also monitored.

The audit trail is displayed in the Recordings dialog. See Figure 37 on page 49 for more information on the audit trail.

Audit Trail Management

When the database table reaches 90% of its possible capacity, VSoIP Lite displays a popup to indicate that the table is nearly full.

Additional popups are displayed every time another 1% of the audit trail is used. Once the table becomes full, VSoIP Lite automatically reduces the table size to the smaller of the following two options:

- Entries for the last 7 days.
- The most recent 10% of entries

Note: During the reduction process, users have read-only access to the system.

Chapter 5 – Recording with VSolP Lite

This chapter contains information on the following:

- Recording Camera Footage
- Recordings Storage Overview
- What Happens When a Partition Becomes Full?
- Playing Back Recorded Video

Recording Camera Footage

VSolP Lite allows you to record continuously from cameras in your surveillance site, or to specify certain times when recording should take place. You can then play back the recorded footage (see “Playing Back Recorded Footage” on page 50).

Note: If you are using a free version of VSolP Lite, you can create up to four recordings. To record more than this, you must upgrade. See “Upgrading VSolP Lite’s Recording Streams” on page 14.

Recordings Storage Overview

In VSolP Lite, you set up partitions during installation. When creating a partition, it is important to take the following factors into consideration:

- **Size** — You should consider the data rate from the camera(s) that will be recording to that partition when deciding on the size (in Gigabytes) of a partition. By choosing a size, you are implicitly specifying the length of recording footage in minutes, hours and days, irrespective of any loop time that may have been specified.

For EACH recorded camera, you should do the following:

- 1 Calculate the bandwidth (in kilobits per second (Kbps)) that the camera is likely to generate as a result of recording the worst case scenario. i.e. lots of motion in the encoded scene, e.g. 1536 Kbps.
- 2 Next, determine how many seconds of footage you wish to record from that camera, e.g. 48 hours = $48 \times 60 \times 60 = 172800$ seconds.
- 3 Obtain the minimum storage requirement for the camera for the required period by multiplying the bandwidth by the required duration, e.g. 1536×172800 , or 265420800 Kb(it). Further convert to gigabytes by first dividing by 8 to obtain a kilobyte value, then by 1024 to obtain a megabyte value, and finally by 1024 again to obtain a gigabyte value, e.g.:
 $265420800 / 8$, or 33177600 KB.
 $33177600 / 1024$, or 32400 MB
 $32400 / 1024$, or approx 32 GB.
- 4 Add a 10% safety margin to the minimum storage requirement, e.g. 32 GB + 3GB, or 35GB.
- 5 Locate a local hard-drive that has sufficient space to satisfy the calculated storage requirement. Do not choose Network Attached Storage (NAS) or any slow speed drive such as a file server share.
- 6 Create a partition for the camera on the chosen drive using a meaningful name, e.g. AccessRampCameraStorage, and enter the calculated storage requirement plus the safety margin of 10%.

Remember to choose the correct partition when scheduling the recording for the camera.

What Happens When a Partition Becomes Full?

When disk space on an Overwrite partition becomes full, VSoIP Lite starts overwriting the oldest recordings on that partition.

When disk space on a Protected partition becomes 90% full, warnings are displayed. You should take action at this point to free up disk space. If disk space levels become critical, a final warning is displayed and recording stops.

Creating a Recording Job

To create a recording job:

- 1 Select the camera that you want to record in the Site Explorer (Figure 35).
- 2 Click Create Schedule.
- 3 Select the required storage partition from the drop-down list.
- 4 Either:
 - Select Continuous Recording to record continuously from the selected camera, or
 - Select Scheduled Recording, and click Show to specify the times when recording should take place.

Note: Do not use this option to set up 24/7 recordings — use the Continuous Recording option.

- 5 Check Loop after if you want the NVR to automatically remove older recordings when they reach a certain age. If you want recordings to be deleted manually by a user with privileges to delete recordings, deselect Loop after.

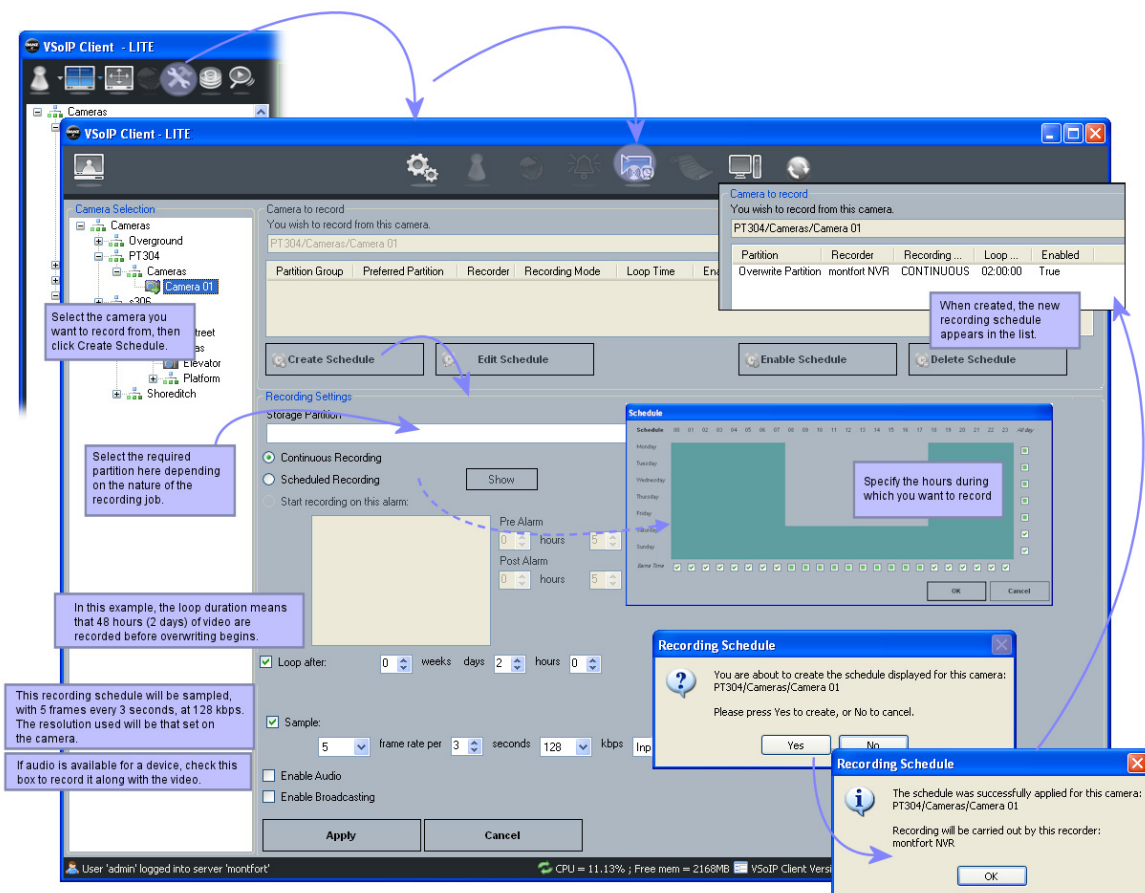


Figure 35 Starting recording from a camera

- 6 If you want to sample the recording stream for this schedule, check Sample, and select the required settings for this stream. For more information on stream sampling, please see “Using Stream Sampling to Reduce Required Storage Space” on page 46.

Note: You can alter existing stream sampling for a schedule, for example, you can change the frames per second setting, but once enabled, you cannot disable sampling for a schedule, and vice versa.

- 7 To record audio (if available on this camera), select Enable Audio.
- 8 Click Apply, then Yes.

Why Can't I Create a Recording Job?

If you get an error message when setting up a recording job, please check the following:

- Ensure that you have not exceeded the number of recording jobs allowed by your NVR license. Note that disabled jobs are included in the total number.
- Check that the device you are trying to record from is online.
- Check that your SQL database has enough space to schedule the recording.

Using Stream Sampling to Reduce Required Storage Space

You may want to record a live video stream, but need to reduce the space required to store the recording. This is known as stream sampling (or sub-sampling). For example, this allows you to reduce the recording impact of a single encoder, megapixel camera without compromising the quality of live video from the camera.

Caution: Stream sampling can greatly reduce the quality of a recording — care must be taken to set the parameters in relation to those of the source to ensure that the resulting recording is viewable.

When creating a recording job, you can alter the input stream by choosing to record a transcoded version of it.

Note: Recordings made of transcoded streams might not be admissible as evidence in court.

- **Frames per second** — Specify how many frames per second of the input stream you want to record. Frames are **not** duplicated to achieve higher frame rates than contained in the input stream.
- **Kilobits per second** — The maximum bit rate that the transcoder can use when transcoding the input stream. A low bit rate will typically reduce image quality especially if the resolution and/or frame rate are high. There is however a limit to how low quality levels can go and this limit MAY be exceeded if the frames per second and resolution are too high.
- **Resolution** — Select the resolution required for the recorded stream. Resolution can be up and down sampled.

For all sample settings, choosing "Input" aims to keep the current characteristic of the input stream as close to that of the input stream as is possible within the constraints caused by the remaining sample settings.

The transcoder will try to achieve the requested resolution. It never duplicates frames, so the FPS setting is only achieved if the input stream's frames per second rate is equal or greater than the frames per second sampling setting. Also, the transcoder aims to stay within the specified bit rate constraints and will reduce image quality to do so.

There is a minimum image quality for sampled recording. If the chosen sampling bit-rate is too low for the characteristics of the input stream, and/or to achieve the sampling settings then the actual sampling bit-rate used will be the lowest one possible, i.e. the chosen setting will not be achieved. If you find the chosen bit-rate sampling setting is unattainable then the recordings could have higher bit-rates than you expect and there will be a reduction in the amount of recording footage that can be stored. In this case consider either increasing the storage area size or reducing the frame rate and/or resolution sampling settings to allow the transcoder to achieve the bit-rate sampling setting chosen.

Caution: Please note that the sustained combined recording and playback bandwidth for each NVR must not exceed 80 -100Mbps. When calculating the combined bandwidth, please take the following into consideration:

- The sum of the bit-rate of each recorded streams irrespective of being sampled or not-sampled
 - The sum of the bit-rate of each playback non-sampled stream (each would be the same as the recorded stream bit-rate)
 - The sum of the bit-rate of each playback sampled stream (each would be according to the bit-rate as a result of the sample settings)
-

Caution: The actual process of transcoding the stream (altering stream parameters) can be very processor-intensive, and care should be taken not to overload the CPU.

Playing Back Recorded Video

VSolP Lite allows users to view up to 4 recordings simultaneously. Recording footage is stored on the integrated NVR which is installed at the same time as VSolP Lite. For information on creating recordings, see “Recording Camera Footage” on page 44.

Note: In this section the term *recorders* is used to mean Networked DVRs or the integrated NVR.

Discovering Recorded Footage

To view recordings for a device, or set of devices, select an item in the tree.

- If you select a single device, (for example, Elevator in Figure 36), only recordings for that camera are shown.
- If you select a device with more than one camera attached (for example, Covert), or a location which has more than one device associated with it (for example, Underground), all recordings for all devices associated with that item are displayed.
- If more than one recording is shown for a single device, this may be due to an NVR failure during the recording. The recording may have switched automatically from one NVR to another. For more information, please see “NVR Failover” on page 132.
- If the camera associated with a recording is no longer available in the site, the recording is still shown in the list, with the Camera Name shown as “Deleted Device”. Recordings made by a recorder no longer in the surveillance site are not listed.

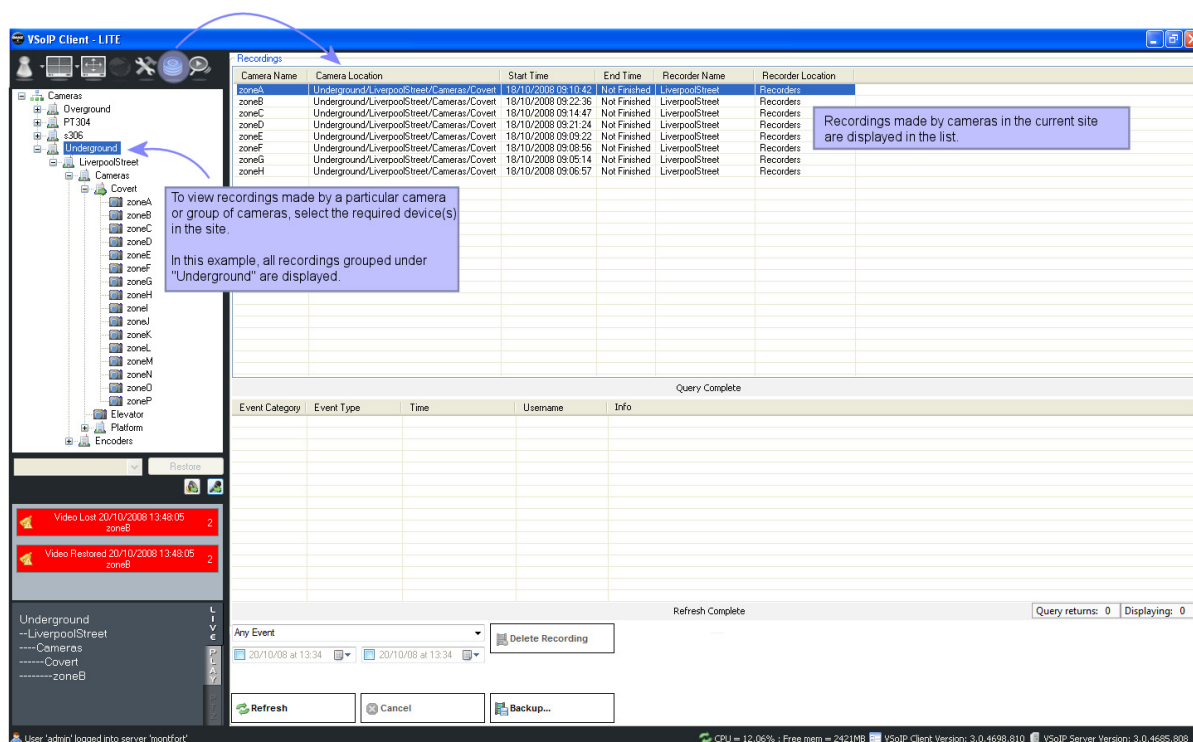


Figure 36 Recordings discovery

Displaying an Events List for a Recording

You may wish to view more information about a particular recording. VSoIP Lite allows you to display all events which occurred while a recording was in progress:

- 1 Display a list of recordings as described above.
- 2 Select a recording in the list.
- 3 Select the type of event you want to display. Select “All events” to display all events which occurred during the recording, including any triggers that are associated with the device that has been recorded.
- 4 In Figure 37, all events which occurred during the recording made by the zoneA camera are displayed.

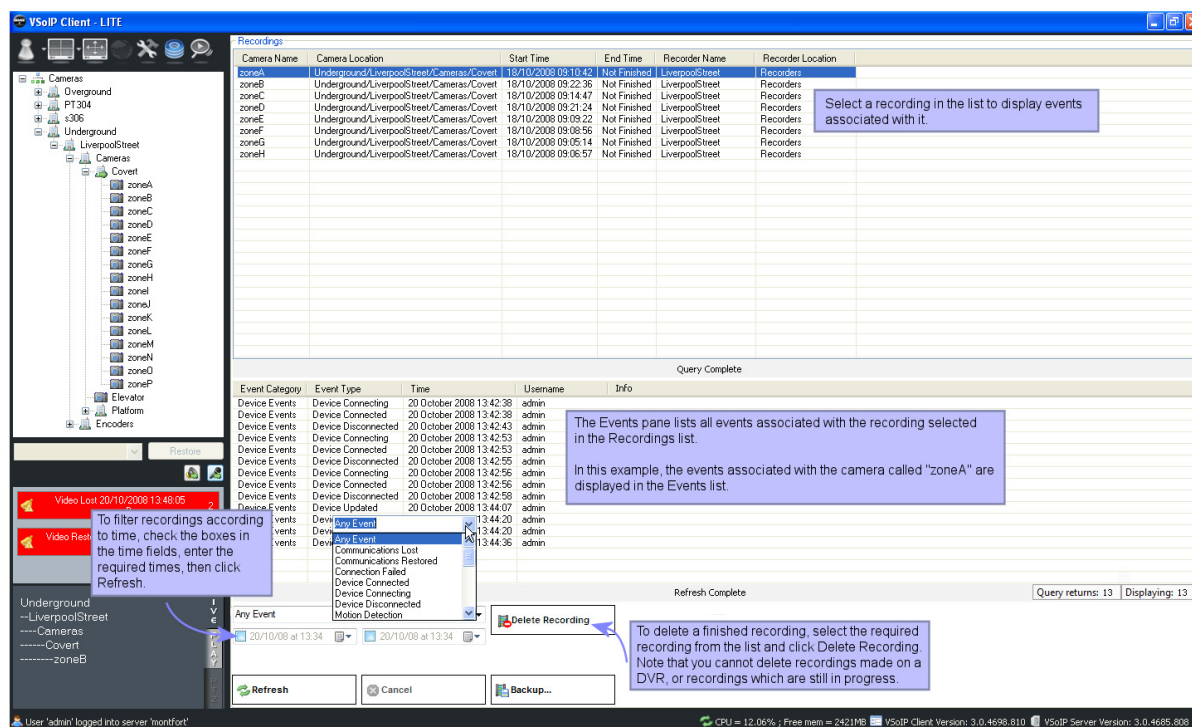


Figure 37 Listing events for a selected recording

- 5 Double-click any of these events to start playing back the recording from the time of the selected event. The recording is displayed in the top-left corner of the recordings window, which switches automatically to a 2x2 layout.

Playing Back Recorded Footage

To play back recorded footage, follow the steps outlined in Figure 38.

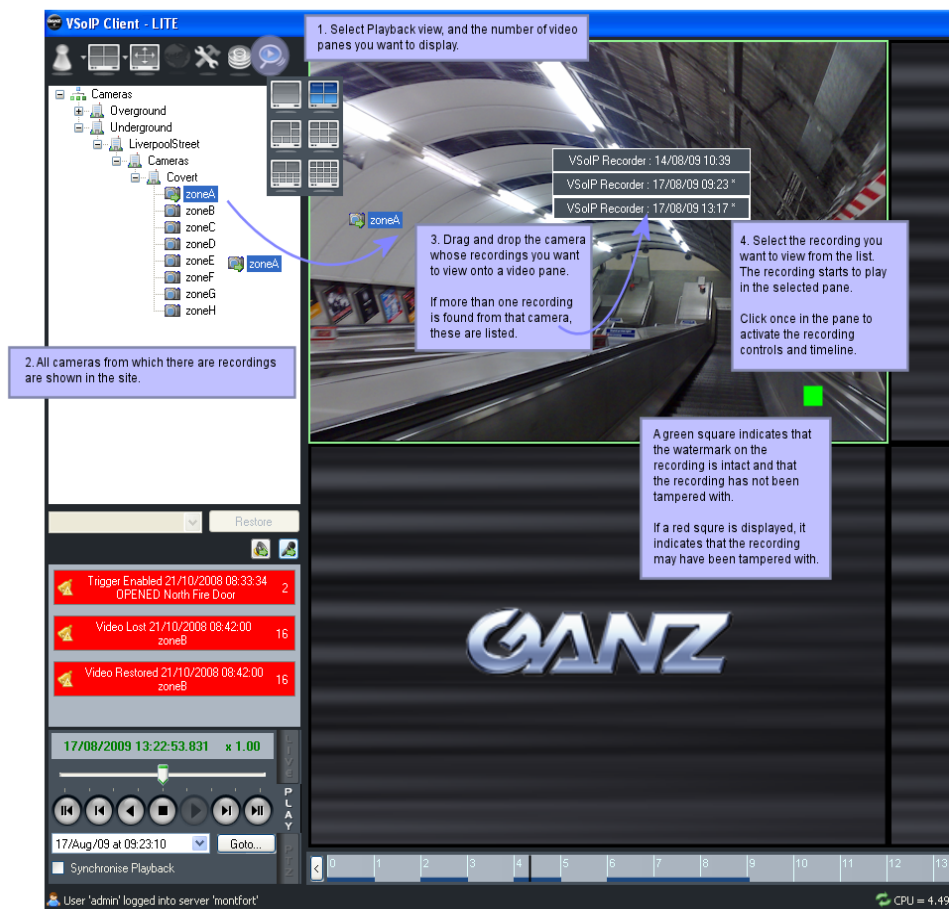


Figure 38 Initial playback and reviewing footage

If your mouse has a scroll button, you can zoom in and out quickly on the timeline. Position your mouse over the area of the timeline you want to view in more detail, and move the scroll button up to zoom in, and down to zoom out.

Playback Controls

Once playback starts, various playback controls are available: rewind, fast forward, pause, resume, step-forward, step-back. Also, the current position is indicated as a date and time.

Note: Not all recorders can perform every playback control, e.g. step-back. If an operation is not possible, the request to perform it is ignored.

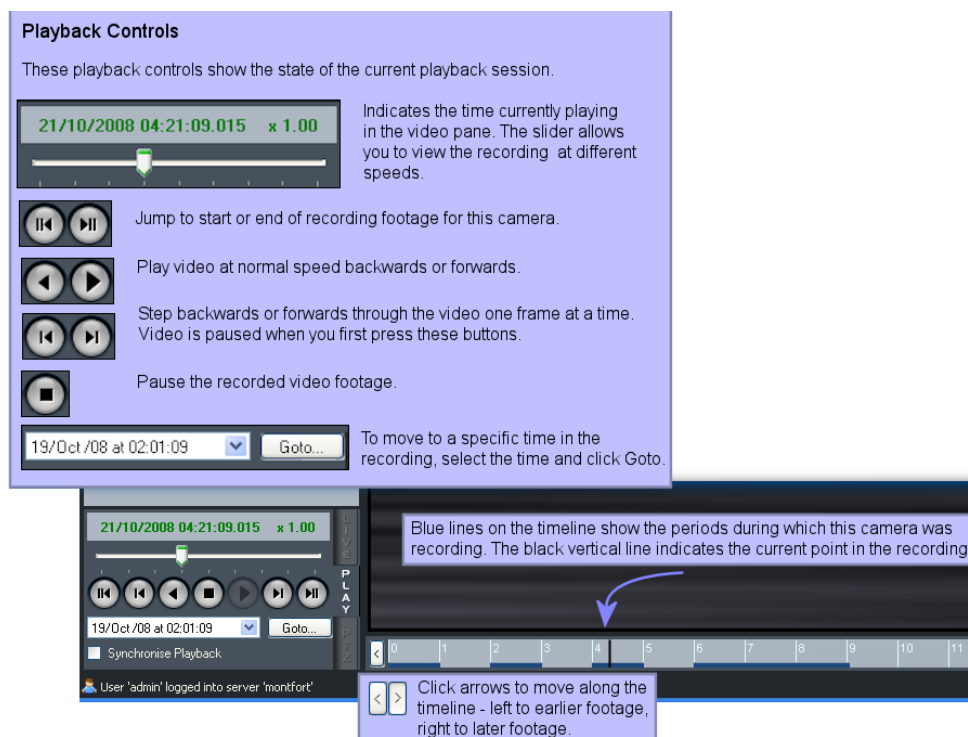


Figure 39 Controlling playback

Using Digital Zoom

VSoIP Lite allows you to zoom in on and move around recorded video footage.

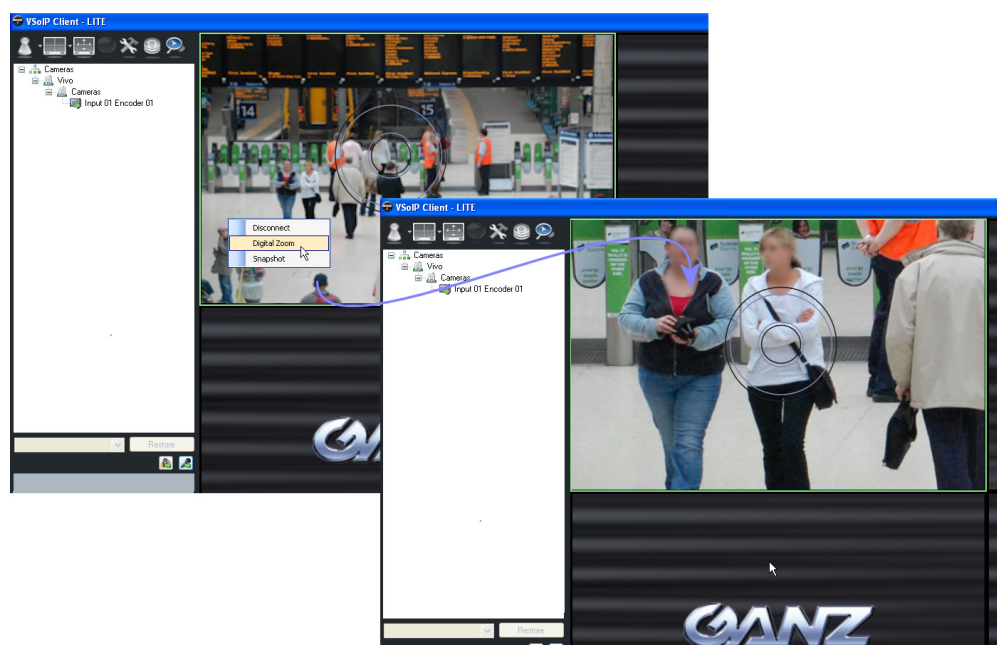


Figure 40 Zooming in to recorded video

Click the part of the video pane that you want to see in more detail, then use the mouse scroll button to zoom in and out as required. While zoomed in, click away from the centre of the image to pan the video.

Taking a Snapshot of Recorded Video

VSolP Lite allows you to capture snapshots of recorded video playing in a video pane. By default, these are saved to \Desktop\VSolP Image Clips\FromRecordings, as .jpeg images.

To take a snapshot, right-click in the pane displaying the video at the point you want to capture, and select Snapshot.

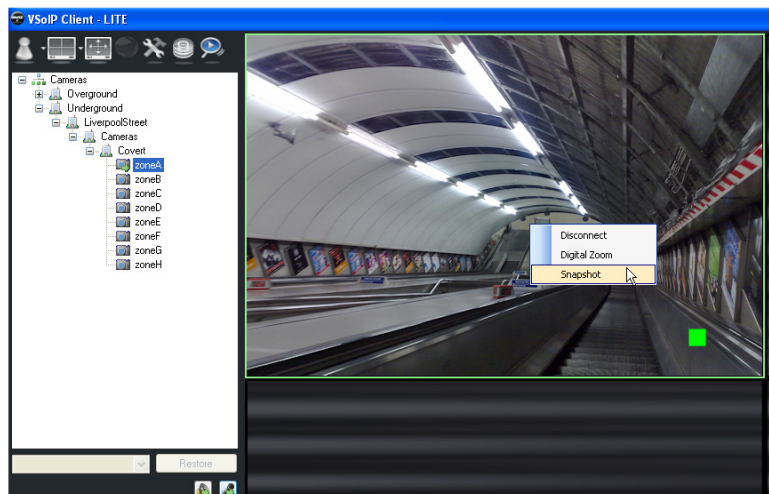


Figure 41 Taking a snapshot of recorded video

Editing Recording Jobs

An existing recording job can be edited to use an alternative set of rules about when to record, e.g. switching on or switching off the looping functionality, or changing the loop duration. The partition on which the recording is being made can also be changed. If the recording job for that video source is no longer required then the recording job can be disabled.

Note: It is not possible to change the video source of a recording job.

Deleting/Disabling Recordings

VSolP Lite automatically starts to overwrite older recordings when the partition on which they are stored becomes full.

However, you can manually delete recordings for a particular camera, as follows:

Due to the internal design of the VSolP Lite NVR, “deleting” a job in the VSolP Lite client *disables* it on the NVR. Remember that you can edit a job to use a different recording criteria, for example, looping policy, and/or storage partition. If the recording job for a video source is no longer required then you should disable it, as shown in Figure 42.

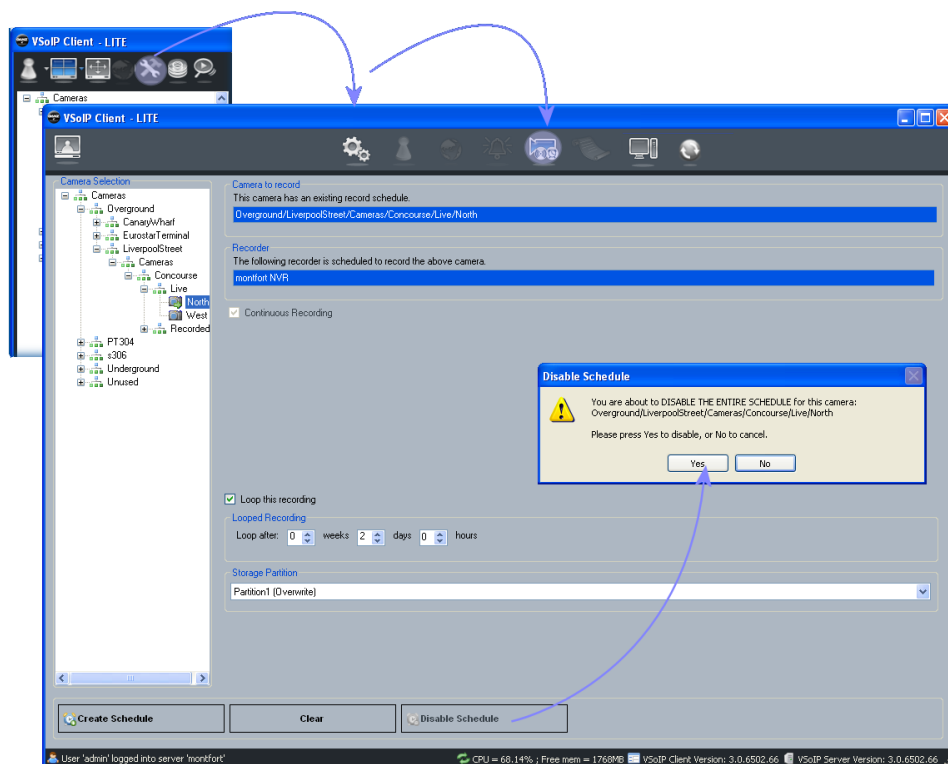


Figure 42 Disabling a recording job

Caution: Please be aware that disabled recording jobs count towards the total number of recording streams.

Synchronising Playback of Recorded Footage

To help operators review recorded footage from multiple cameras on multiple networked DVRs and/or the integrated NVR simultaneously, it is possible to control playback using a master set of playback controls. This allows playback to be paused and “wound” forward or backwards at the same time saving time switching between playback sessions.

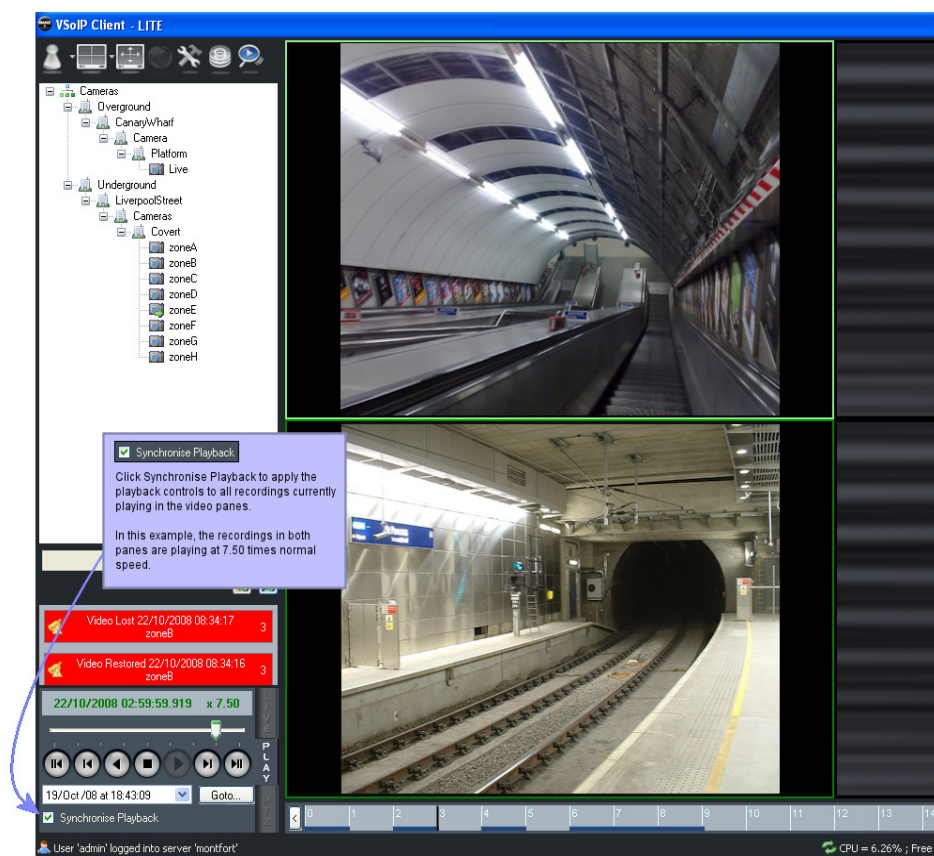


Figure 43 Synchronised playback

Note: Networked DVRs can vary in their performance. Some are limited to a certain number of concurrent playback sessions. The performance of the application during synchronised playback will reflect the responsiveness and performance of the poorest responding and performing element.

Exporting Recorded Video

For evidential purposes, it is often necessary to extract a portion of recorded footage for playback in a player application. Locate your recording in the list of recordings of IP cameras and camera inputs on Networked DVRs.

Figure 44 shows the steps required to export recording footage.

Note: If the recording has audio associated with it, you can choose to export just the video, or video with audio. Note that audio can only be exported in native mode, not in MP4 format (see “VSolP Export Player” on page 55).

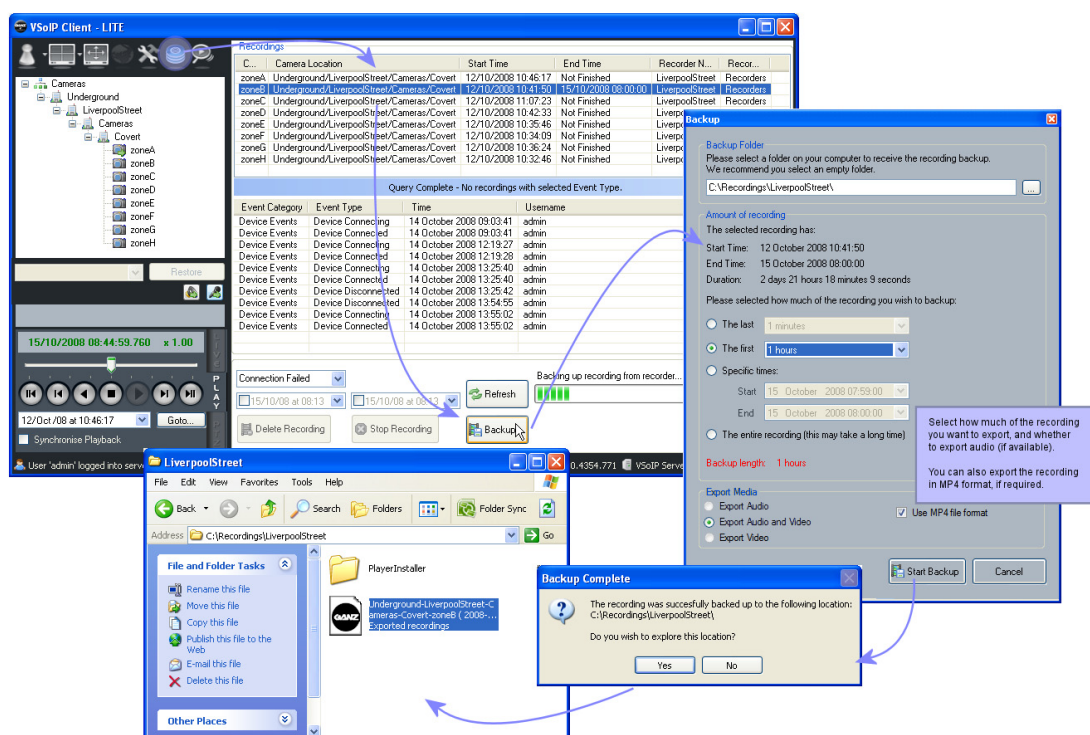


Figure 44 Exporting recording footage

Note: When you select video footage to export, VSolP Lite checks the integrity of the selected video and informs you if the export is likely to encounter problems.

VSolP Export Player

VSolP Export Player is designed to maintain the evidential integrity of the original recording by keeping the recording in its native format. Unlike other forms of export, e.g. MP4, native exporting means that the exported recording has not been transcoded or altered in any way.

When VSolP Lite is instructed to export recordings in native format, it copies the Exported Recordings Player Installer into the same folder as the exported recordings. The folder therefore contains one, or more, .REX files - one for each exported recording and the installation program for the player. The intent is to create an evidence “pack” for use by individuals without access to VSolP Lite.

Note: Although the computer running VSolP Export Player can be considered to be a general purpose PC, it must support Microsoft Direct-X 3D rendering to a reasonable performance level.

For information on using VSolP Export Player, please see the VSolP Export Player User Guide.

Chapter 6 – System Administration

This chapter contains information on the following:

- Restoring Factory Defaults
- Viewing System Information
- Default Settings

Restoring Factory Defaults

You can revert VSoIP Lite back to its factory default settings, as shown in Figure 45:

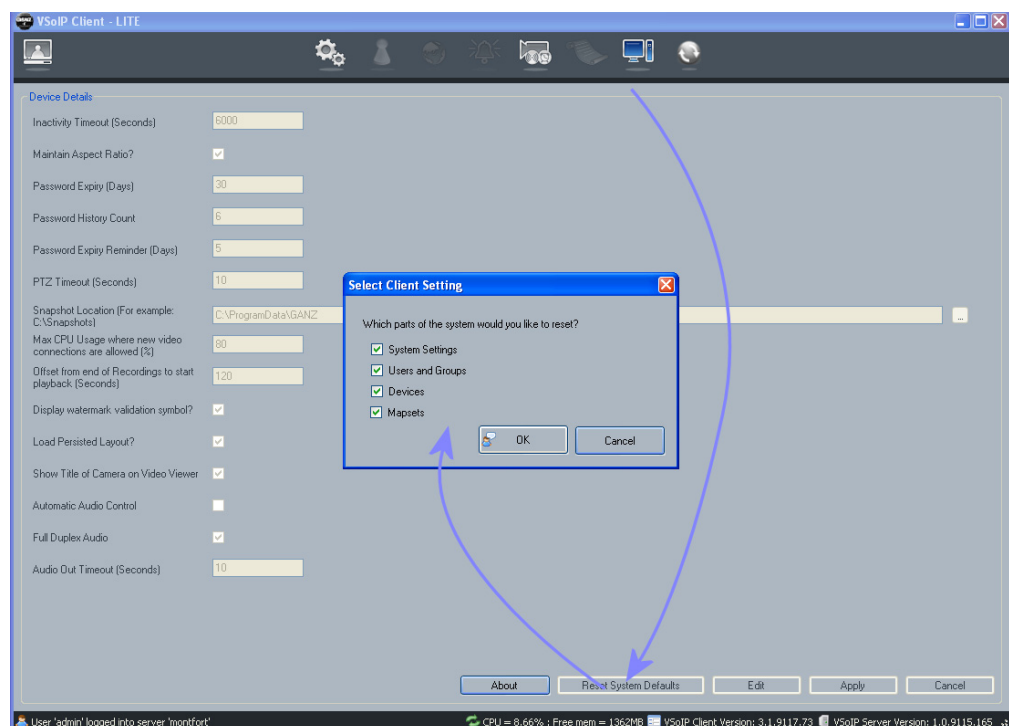


Figure 45 Restoring factory defaults

Select which parts of the system you want to reset, and click OK.

Caution: It is not possible to undo this action, so ensure that you really want to reset the settings before proceeding.

Note: After restoring to factory defaults, you must restart VSoIP Lite to have access to full functionality.

Viewing System Information

You can view details of the current installation of VSoIP Lite, as shown in Figure 46:

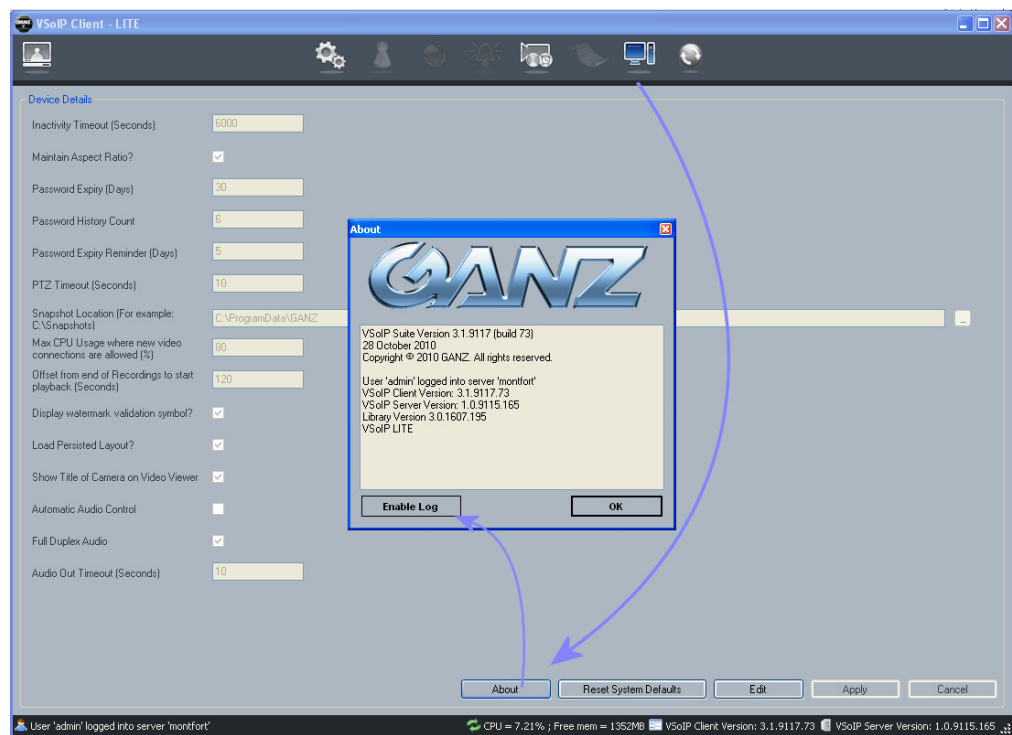


Figure 46 Viewing installation details

Default Settings

VSolP Lite allows you to change certain system settings. Figure 47 shows how to view these settings, and change them if required.

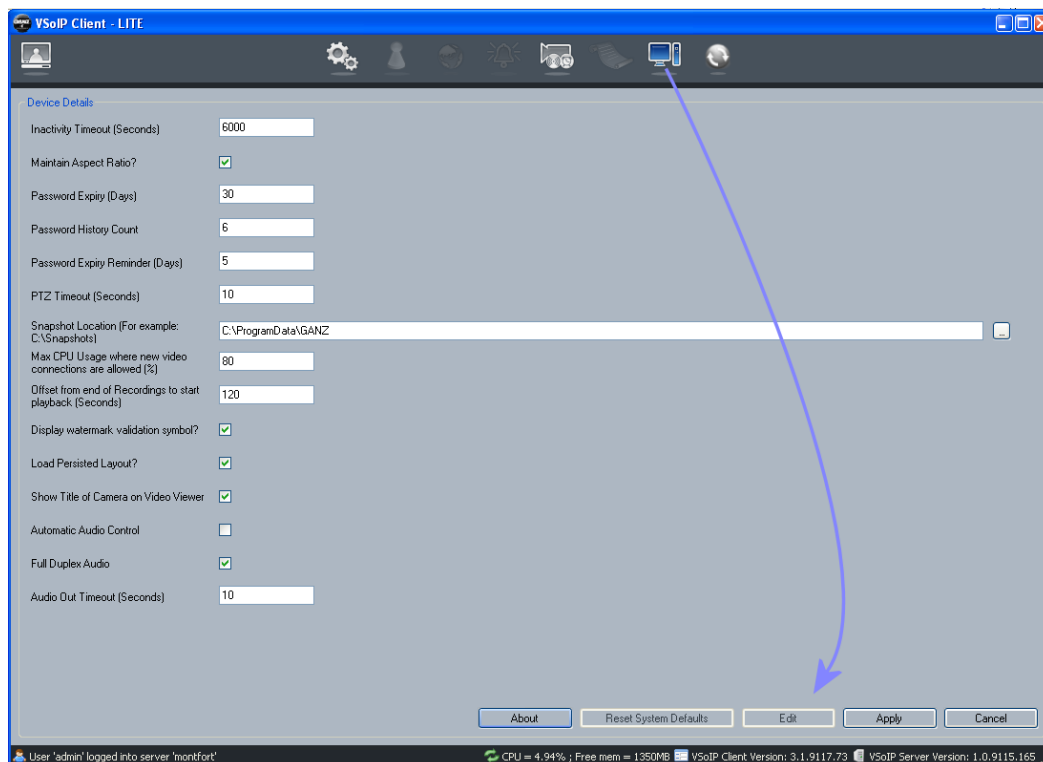


Figure 47 Viewing existing settings

Table 9 Available VSolP Lite settings

Setting	Meaning	Default Value
Inactivity Timeout	Length of time that the client can be inactive before a password is required to access functionality again. Setting this value to zero means that the client never times out.	600 seconds
Maintain Aspect Ratio	Maintain correct aspect ratio of video panes, even when they are resized.	On
Password Expiry	Length of time before a password expires and must be changed.	30 days
Password History Count	The number of different passwords that must be used before a password can be reused.	6
Password Expiry Reminder	The number of days before a password expires that you are reminded to change it.	5
PTZ Timeout	Length of time that a PTZ camera can be inactive in a video pane before the PTZ controls must be reactivated.	10 seconds
Snapshot Location	The folder where snapshots from live and recorded video are stored. VSolP Lite automatically creates separate sub-folders for live and recorded snapshots. Note: This is the path on the computer running the client software component rather than a path on the computer running the server.	C:\WINDOWS\system32\config\systemprofile\Desktop
Max CPU Usage	The maximum CPU usage at which new video connections are allowed. This prevents overdriving the system by preventing new connections starting when the current displayed video is consuming more than this maximum value.	80%
Playback Offset Time	When playing back a recording by dragging and dropping it onto a playback pane, this is the number of seconds before the current time at which video starts playing, for example, now, minus 120 secs.	120 seconds
Show Watermark	Specify whether a red or green square is displayed on recorded video to indicate the integrity (or not) of a recording.	On

Table 9 Available VSoIP Lite settings (Continued)

Setting	Meaning	Default Value
Load Persisted Layout	When opening the application, display the same cameras and layout that were in use when the application shut down.	On
Show Title of Camera in Video Viewer	Display the camera name (and path) on the top left of video panes which are displaying live video. Note: This setting does not apply to video displayed in the client via a Video-wall. For information on how to display overlays on a Video-wall itself, see the Video-wall User Manual.	On
Automatic Audio Control	When interacting with a device that supports audio, this option allows a user to hear audio from a camera by clicking on the pane in which it is displayed. For more information, see “Listening to Audio from a Camera” on page 30.	Enabled
Full Duplex Audio	Allows communications in both directions simultaneously. Disable this option to enable Half-Duplex mode.	Enabled
Audio Out Timeout	This value specifies how long a microphone can be used for before the connection times out	10 seconds

Appendix A – Maintenance Information

The follow section provides useful information regarding the general use and setup of the surveillance system.

Opening a Command Prompt in Microsoft Windows

The command prompt allows certain tools that do not have a graphical user interface to execute. Often such commands require extra parts, called arguments, that detail what options need to be configured.

For instance, the networking command `ping` allows the network connections to another networked device to be tested. The main argument required is the IP address of the device, e.g. `ping 10.11.12.13`

Note: Often the commands executed at the command prompt require certain privileges, therefore it is important to use the command prompt as an administrator level user.

Windows XP

To access the command prompt, click Start menu>All Programs>Accessories>Command Prompt. It is also often started from the Run dialog (see below) by typing `cmd` and clicking OK.

In the command prompt window, enter the required command at the prompt after the `>` character. After typing the command, press Enter to perform the command.

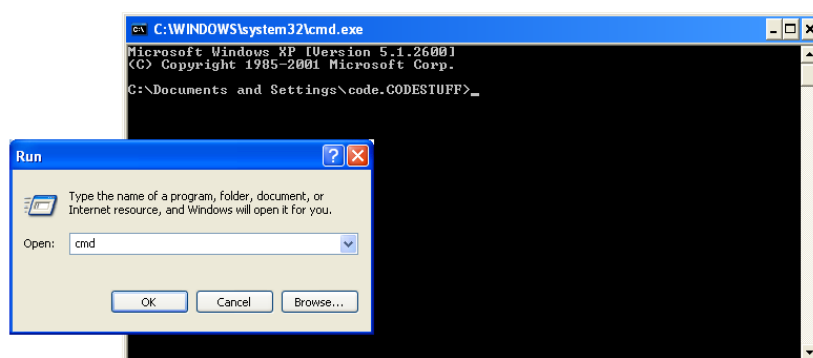


Figure 48 Opening a Windows command prompt

Opening the Run dialog

To open the run dialog, either:

- Select Start>Run, or
- Hold the Windows key and press the “R” key.

Note: If the Start menu item Start>Run is missing you can enable it by right-clicking the Start menu button. Choose Properties, select the Start Menu tab, click Customize then select the Advanced tab. In the Start menu items list-box, locate the Run command entry and check the box against it. Click OK twice to apply the change.

Finding out the IP Address of Your Computer

There are a number of ways to do this. One approach that can be relied on irrespective of the Windows version being used is the command `ipconfig`.

To use `ipconfig`, open a command-prompt. Enter the command `ipconfig`. On entering the command, the operating system will respond with a series of addresses, note the one labelled IP Address.

Determining PC Port Usage

The Windows `netstat` command can be used to list all the network ports that are currently in use on a PC. To use `netstat`, first open a command prompt (see above), then type the `netstat` command as follows:

```
netstat -a -b
```

The command outputs a table with four columns Protocol, Local Address, Foreign Address and state. A large amount of text is generated by this command making it difficult to locate an entry. To assist in locating a particular port save the output of the command to a file using console redirection, e.g.

```
netstat -a -b > c:\portresults.txt
```

The arrow character requests that Windows not show the results on screen but instead puts the results into a file called `portresults.txt` at the root of the C drive.

Once the prompt returns, the command has complete, and the file content is ready to review. Use Windows notepad to view the contents of the results file. Use the find function in Notepad (Edit>Find) to find occurrences of number sequence, e.g. 8080. Remember that `netstat` requests the operating system to list all the ports in use so if port 8080 cannot be found by Notepad then port 8080 is free to use. If the sequence 8080 is found then that port might be in use, further analysis of the line containing the sequence 8080 is required to be certain.

If the 8080 sequence is shown under the third column - "Foreign Address" - then this line can be ignored and the search continued. Also ignore any line found that contains 8080 embedded in another number, e.g. 128080.

If line contains 8080, and the port number is not embedded in another number and the port number is under the "Local Address" column then examine the line immediately below the line to discover what application or service is using this port.

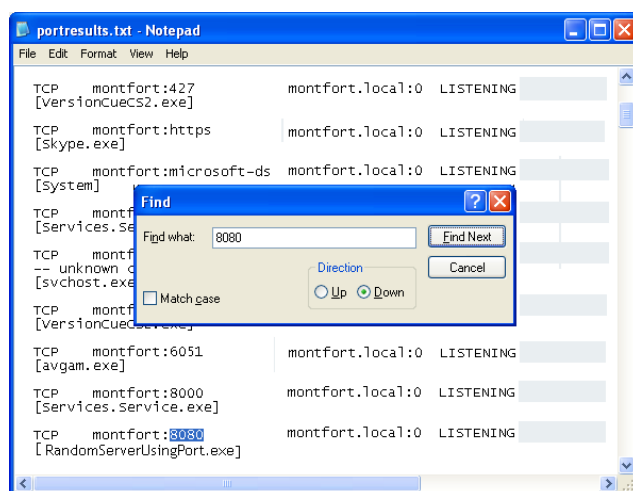


Figure 49 Determining port usage using the `netstat` command

The example shows viewing in Windows Notepad, the result of running the `netstat` command in a Windows Console and using console redirection to create a file containing a list of ports in use. The Find Notepad operation has been used to locate a line containing 8080, in the local address column, and the line after shows that the port is being used by an application called `RandomServerUsingPort.exe`.

Windows Events – Using the Event Viewer

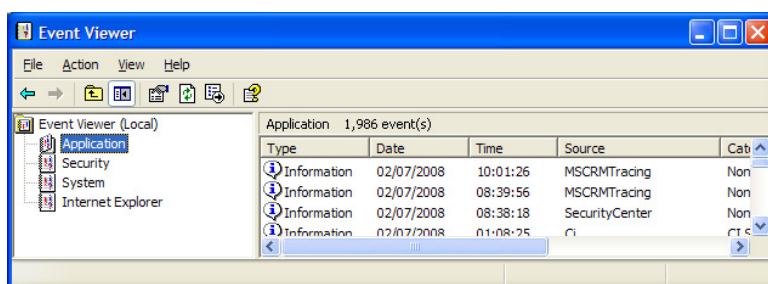


Figure 50 Windows Event Viewer

Some services and applications running on a computer need to communicate with the user but do not have a graphical interface to do so. For these services and applications the operating system provides methods of recording the occurrence of an event. All the events in the system are stored in various event logs. The Event Viewer is a convenient method of examining all events which have occurred recently. Issues concerning the proper functioning of the system are recorded and allow problems to be solved during commissioning and maintenance cycles.

Viewing Windows Logs

The Windows Event Viewer allows you to view various Windows logs. For a surveillance system, the most relevant log is the Application Log. The Application Log stores a historical list of information, warning and error messages related to applications running on the local computer.

To access this log, open the Control Panel from the Start menu and choose Administrative Tools. If the Control Panel is in category view, choose the Performance and Maintenance category, then Administrative Tools. Open the Event Viewer. Double-click the Application log.

When examining the log, note the Source column. This lists the name of the application that generated the log entry. Entries can be:

- Informational, shown with an i icon.
- Warnings, shown with an exclamation mark icon.
- Severe error, shown with a stop-sign icon.

Surveillance suite software components that have warning or error log entries should be read to determine the source of the error. The system log can be useful for finding out about computer issues that might affect the surveillance suite applications indirectly, for example low disk space.

Note: If the Control Panel entry is missing you can enable it by right-clicking the Start menu button. Choose Properties, select the Start Menu tab, click Customize then select the Advanced tab. In the Start menu items list-box locate the Control Panel entry and choose either Display as a link or Display as a menu. Click OK twice to apply the change.

Displaying Hidden or System Files

Windows XP

By default, Windows Explorer does not show hidden or system files. Because of this, you may be unable to see certain files, even though they exist on the drive.

To show hidden or system files in Windows XP:

- 1 Open Windows Explorer, open the Tools menu and choose Folder Options. In the Folder Options dialog, select the View tab
- 2 Under the Hidden files and folders section select the radio button labeled Show hidden files and folders.
- 3 Uncheck Hide extensions for known file types.
- 4 Uncheck Hide protected operating system files.
- 5 Click Apply and then OK.

Windows Vista

To enable the viewing of hidden and protected system files in Windows Vista please follow these steps:

- 1 Click Start>Control Panel menu option. When the control panel opens you can either be in Classic View or Control Panel Home view.

If you are in the Classic View do the following:

- a. Double-click on the Folder Options icon.
- b. Click on the View tab.
- c. Go to step 2.

If you are in the Control Panel Home view do the following:

- a. Click Appearance and Personalization.
- b. Click Show Hidden Files or Folders.
- c. Go to step 2.

- 2 Under the Hidden files and folders section select the radio button labeled Show hidden files and folders.
- 3 Uncheck Hide extensions for known file types.
- 4 Uncheck Hide protected operating system files. Once this is done, your Folder Options screen should look similar to the following image.

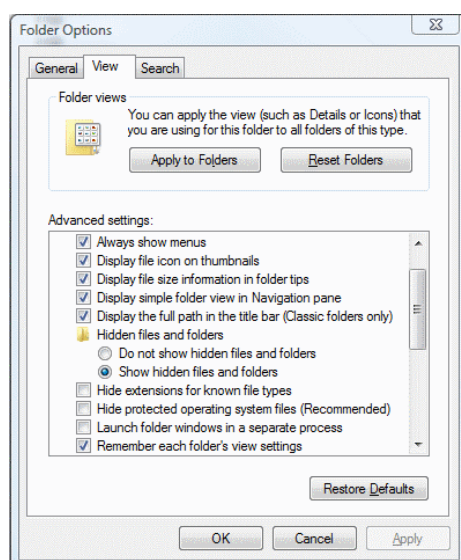


Figure 51 Showing hidden files and folders

- 5 Click Apply and then OK.

Windows 7

If the Windows Search service is enabled on your PC, please follow these steps to enable the viewing of hidden and protected system files in Windows 7:

- 1 Click the Start menu button and enter "hidden" in the search programs and files box.
- 2 Locate and click the "Show hidden files and folders" item in the list.
- 3 Select Show hidden files, folders and drives (see Figure 51).
- 4 Click Apply and then click OK.

If the Windows Search service is disabled, please follow these steps:

- 1 Click Start>Control Panel menu option.
- 2 Select Appearance and Personalization, then under Folder Options, select Show hidden files and folders.

- 3 Under the Hidden files and folders section select the radio button labeled Show hidden files and folders.
- 4 Uncheck Hide extensions for known file types.
- 5 Uncheck Hide protected operating system files. Once this is done, your Folder Options screen should look similar to Figure 51.
- 6 Click Apply, then OK.

Configuring Application Log to Overwrite Oldest Entries

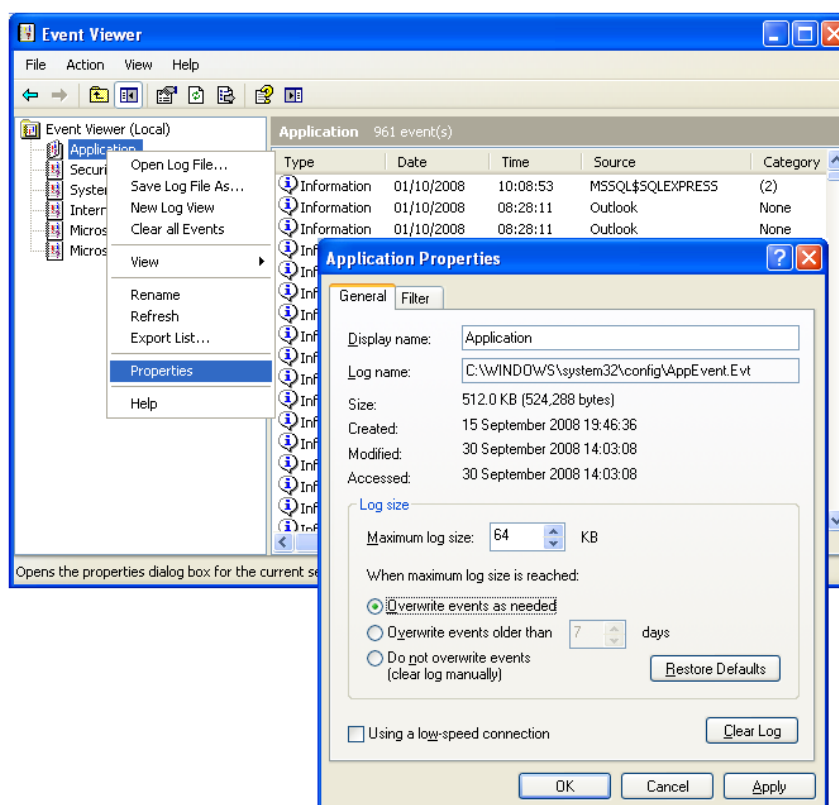


Figure 52 Changing Windows logging behaviour

The Event Log can become full and prevent proper execution of the tasks running on the computer. To prevent this, change the properties of the application event log to overwrite earliest events when there is insufficient space available.

To do this:

- 1 From the Start menu open the Control Panel and choose the Administrative Tools. (If the control panel is in category view, choose the Performance and Maintenance category, then Administrative Tools.)
- 2 Open the Event Viewer.
- 3 Double-click the Application log.
- 4 Right-click the Application entry in the left-hand window and choose Properties.
- 5 In the Application Properties choose the General tab and in the Log size group click Overwrite events as needed, and click OK.

Viewing Windows Services List

Some parts of the surveillance system run as background tasks and do not require a user to be logged in for tasks to be run. These background tasks are known as services.

Although services run in the background, do not interact with users graphically, and do not require a user to be logged in, they are initiated, run and owned by a user account on the computer. Typically this account is one of the built-in accounts, usually a user called LocalService or sometimes a user called NetworkService.

Services can be automatically started or stopped by the operating system when it starts or shuts down. Alternatively, they can be manually started or stopped by a logged in user with sufficient privileges to do so.

When service-based surveillance suite components are installed, they are installed in a state that requires a logged-in user with appropriate privileges to start the service.

The Windows Services list permits a logged-in user with sufficient privileges to:

- Switch a manual service to start automatically.
- Switch an automatically starting service to manual
- Completely disable the service, preventing it from being started.

To open the Services list, from the Start menu open the Control Panel and choose the Administrative Tools option. If the Control Panel is in category view, choose the Performance and Maintenance category, then Administrative Tools. Open the Services application.

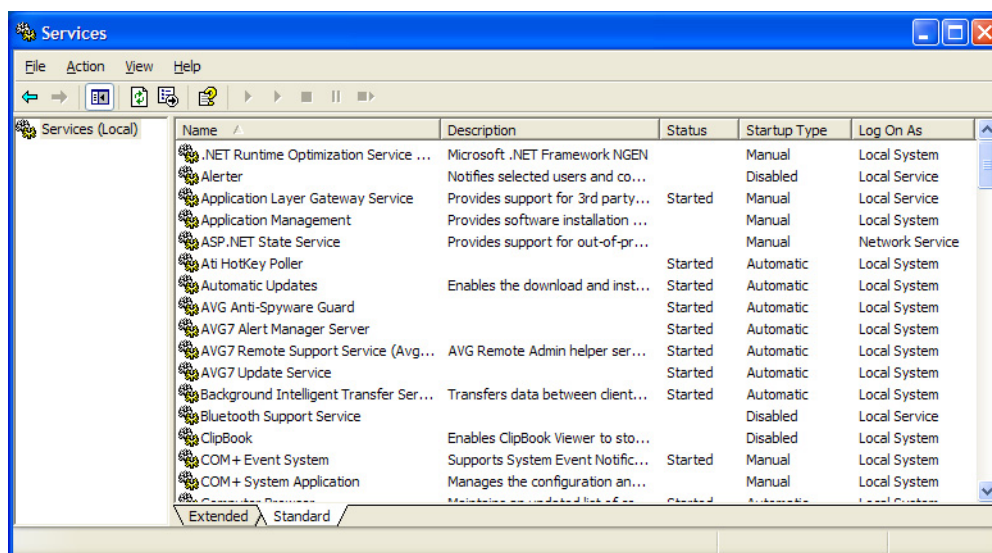


Figure 53 Windows services application

Right-click and choose Properties to display the Properties dialog for the service.

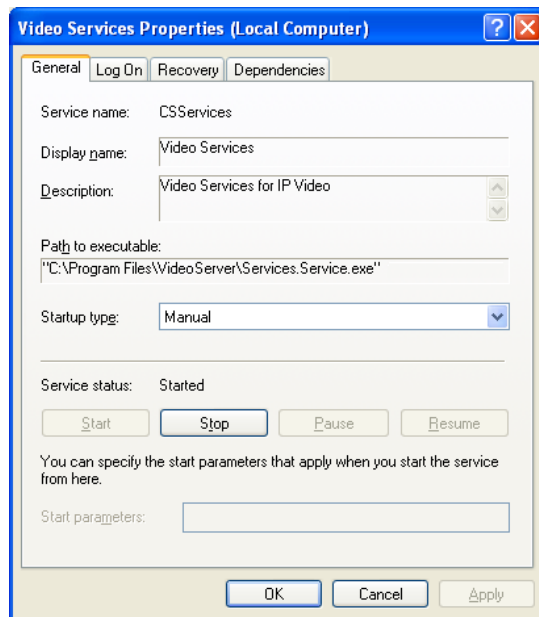


Figure 54 Configuring start-up action for selected service

To request that Windows start a service when the operating system starts, change the Start-up type to Automatic. Note that the service will not actually start until Windows is re-started. To start the service from this dialog, select the required service and click Start.

To change an automatic service back to one that requires a logged-in user to start and stop the service, change the Start-up type to Manual. Note that a started service will not stop until Windows is shut down. To stop the service before then, select it in the list and click Stop.

Note: Informational messages, warnings and error events logged by services can be viewed through the Windows Event Viewer.

Checking Connectivity of a Networked Device or Computer

During installation, commissioning and when troubleshooting an installed system, it may be necessary to confirm that a particular network device is reachable. One technique is to use a network ping. This sends a special data packet over the network that the end party replies to, once received. Unless configured not to, most networked devices, IP cameras, Networked DVRs, computers running a server component, computers running a NVR component or computers running a Video-wall component will reply to incoming ping requests.

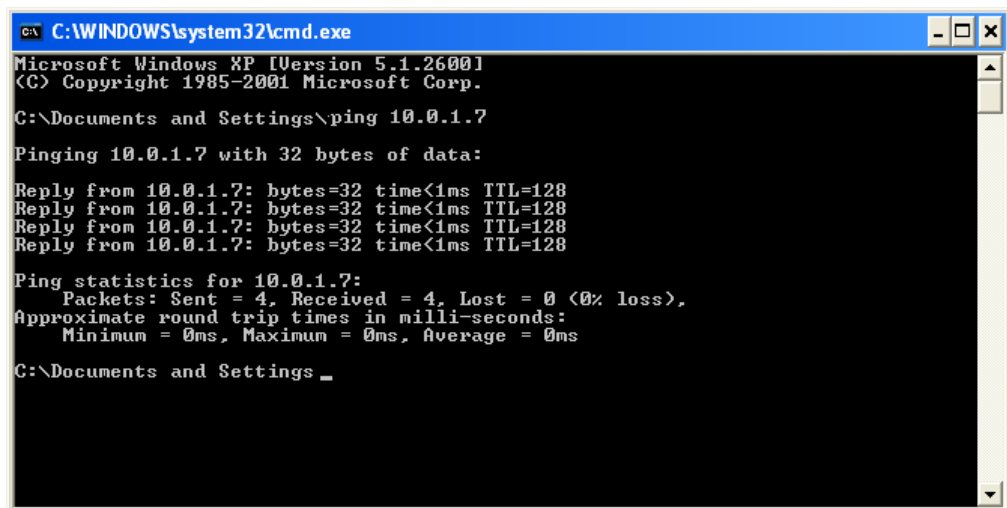
To use a network ping you need to know the IP address of the network device you wish to find.

Note: If no response is received from a pinged network device then first ensure you have the correct IP address for the device. If this is correct, then confirm that you have connectivity with other network devices before assuming that the device is not reachable. It might be that the computer from which you are issuing the ping is not able to reach some, or all networked devices due to a configuration issue with the computer you are using, a coincidental localised or wider network-connectivity issue, or the presence of a software firewall preventing ping requests being sent or received.

Sending a Ping

The following steps show how to determine whether a certain device with IP address 10.0.1.7 is available on the network. It assumes that some checks have been made to ensure that the computer being used in the test is connected to the same network as the device, and that other devices known to exist and connected to the network have responded.

- 1 Open a Command prompt.
- 2 Type `ping 10.0.1.7` and press Enter.
- 3 If the network device (or computer running a surveillance software component) cannot be reached then the response will be at least 4 lines indicating "Request timed out".

A screenshot of a Windows XP command prompt window. The title bar reads 'C:\WINDOWS\system32\cmd.exe'. The window content shows the following text:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ping 10.0.1.7

Pinging 10.0.1.7 with 32 bytes of data:

Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128
Reply from 10.0.1.7: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings _
```

Figure 55 Successful ping reply

- If the network device was reachable then the response will contain several replies.
- If there is a mix of replies and timed out messages, this suggests that a network connection fault exists, that the network is highly congested, that the target device is too busy due to heavy workload to reply, or a mixture of these. In this case, this indicates that there is a system issue which could adversely affect the system's overall performance and could result in failed recordings, live or playback requests, and a general lack of system responsiveness.

The ping command is a useful troubleshooting tool that can highlight issues affecting the overall system and is one method that might indicate that the overall system is currently overdriven and is not operating as designed.

Troubleshooting

Troubleshooting is a complex area when the components of the surveillance suite software, the underlying operating systems, database managers, rendering engines, the different types of hardware involved and the various issues related to networking are all taken into consideration.

This section covers some typical issues that occur when installing, running and maintaining the surveillance system. It also describes how to assist a technical support representative by providing them with useful information and run-time log files to help them determine the root of a problem. It is worth noting that by examining the information provided there will be cases where the solution might be obvious and you can implement a solution without having to contact the software vendor or other support provider.

It is important to note that a high level of technical competency is required in order to perform troubleshooting. There are a number of skills required to identify the likely cause of the issues being experienced and several attempts might be required to solve problems.

It is very important to design a system from the outset rather than to make an arbitrary system using various hardware elements and using networking infrastructure that has not been optimised for surveillance use, i.e. not high bandwidth optimised. There are discussions elsewhere about the importance of design in constructing the surveillance system.

Note: It is assumed that the overall system (software, hardware and networking infrastructure) is fit for purpose and has performance safety margins that allow peaks of demand to be accommodated. It is also assumed that high performance computer hardware is used: server grade for server and Networked Video Recorder components and that all computer hardware matches or, preferably, exceeds the minimum specifications.

Caution: It is highly recommended that computer hardware is NOT used to perform non-surveillance system tasks unless the interaction between the CCTV and non-CCTV aspects of the installation can be safely accommodated within the specification of the computer and there is no shared dependency, e.g. shared database manager usage, that compromises the system.

Providing Technical Support Information

All software components have a built-in automatic log file generator. The generator is enabled whenever a special file called logging.config is detected.

Enabling Logging

To enable logging:

- 1 Click the System Settings icon as shown in Figure 56:

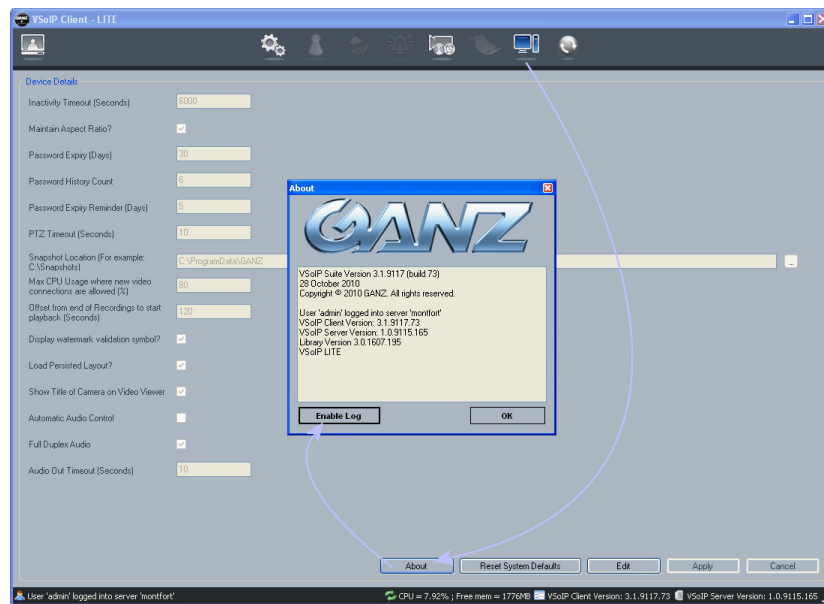


Figure 56 Enabling logging

- 2 Click Enable Log. This creates a file called logging.config in the installation folder. Reading the log file can be useful for understanding whether Networked DVRs, IP cameras and encoders are communicating successfully with the client, server and recorder software components.

Alternatively, you can enable logging manually, as follows:

- 1 Locate a suitable logging.config file and copy it into the clipboard. This will be:
 - In the installation folder of the software component and called logging.config.disabled (or some other name that distinguishes it from logging.config), or
 - In a sub-folder of the installation folder.

Alternatively, you might be sent the file by a technical support representative.

- 2 Close the application you want to log.
 - For clients, exit the application.
 - For servers or NVR components, stop the service controlling the application.
- 3 If necessary, paste the logging.config file into the installation folder. (If necessary, rename it so that it is called logging.config.)
- 4 Start the application to be logged.
- 5 Note that a log-roll.txt file will appear in one of the following locations, depending on your operating system: (the following examples are for the Client)

- Vista/Windows 7: C:\Program Data\CSLogging\VSolPCClient
- Windows XP/Server 2003: C:\Documents and Settings\All Users\CSLogging\VSolPCClient

Disabling Logging

To disable logging:

- 1 Click the System Settings icon.
- 2 Click Disable Log. The file logging.config is automatically deleted from the installation folder.

Alternatively, you can disable logging as follows:

- 1 Close the application currently being logged.
 - For clients, exit the application.
 - For servers or NVR components, stop the service controlling the application.

Note: Currently the application being logged will occasionally write to the log-roll.txt file. You will not be able to delete the log-roll file(s) or the logging.config file until the application being logged is stopped.

- 2 Remove the logging.config file from the installation folder by moving to a sub-folder, to another safe location, deleting it (if you have kept a copy) or renaming it to (for example) logging.config.disabled.
- 3 Start the application.
- 4 Note that after removing any log files, no more log files are added to the folder.

How Logging Works

Caution: The logging.config file contains the operating parameters for the generator and should not be modified unless you have been instructed to do so.

The log file generator automatically "rolls" the log file every hour. This means that the log-roll.txt file is renamed to a name starting with log-roll but also appends the date and hour of the day that the log started on, and a new log-roll.txt file is created containing the next hour's logging information.

This rolling behaviour has two undesirable side effects:

- When the application being logged is restarted, the log-roll.txt is deleted and a new one created. This may mean that vital error information gathered prior to the failure of the application is lost.

To overcome this and capture the last moments of an application's behaviour in the log file, locate the log-roll.txt and rename it to, for example, log-roll-showing-UAE.txt. This means when the application being logged is restarted, the log-roll.txt will not be present to be overwritten.

Note: If the application is still executing and you wish to capture the moment when something happens, wait until the required moment has passed, then stop the application. Once stopped, rename the log-roll.txt file as described above, and restart the application.

- If logging is enabled and the system unmaintained for an extended period, the log files may eventually consume large quantities of storage on the drive where the application is installed. This could compromise the overall performance of the computer running the application being logged.

To overcome this, you can safely move or delete log-roll files with dates and times appended to the file's name, since these are not actively being written to by the generator. Alternatively, be sure to disable logging once your logging requirements have been met.

Caution: Logging puts extra demand on any system due to the CPU load of executing surveillance software components and log generator. This could cause system overload and result in misleading log content.

In some cases where overall system power is limited, enabling logging can put a serious load on the system, perhaps causing the system to become overdriven. Always ensure that the computer is able to accommodate the logging overhead on top of normal system operation. If this is not done, the content of the logs may be misleading since they will reveal an overdriven system rather than the fault trying to be captured. In such situations alternative approaches to troubleshooting are required.

Specifying the Logging Level

There are five logging levels:

- Debug
- Info
- Warn
- Error
- Fatal

Each logging message is assigned a level of importance, and these are reflected in these levels. For example, Debug stores **all** logging messages, whereas Fatal only stores application-critical logging messages. By default, the logging level is set to Warn.

To change the level of logging, edit the logging.config file as follows:

- 1 Open logging.conf in Notepad or another text editor.
- 2 Search for the string: `<level value="WARN" />`
- 3 Change the WARN parameter to one of the above levels, for example, `<level value="FATAL" />`.
- 4 Save the file.

Appendix B – Supported Devices

This appendix provides a list of devices currently supported by VSolP Lite.

Device Model	Device Type	Alarm Inputs	Alarm Outputs	Direct PTZ	Transparent PTZ	Motion Detector	NVR Recording	DVR Recording/Playback	Videowall Live Display	Encoders	Audio	Remote Config
ZN-T9000	MPEG4 Videoserver	4x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-C9000	MPEG4 CS-mount camera	4x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-T8000	MPEG4 Videoserver	2x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-C8000	MPEG4 CS-mount camera	2x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-D9000	MPEG4 dome camera	TBI	TBI	N/A	N/A	TBI	YES	N/A	YES	1	NO	by I.E.
MP1AI	M-JPEG C-mount camera	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	NO	**
MP2AI	M-JPEG C-mount camera	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	NO	**
MP3AI	M-JPEG C-mount camera	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	NO	**
MP5AI	M-JPEG C-mount camera	N/A	N/A	N/A	N/A	TBI	YES	N/A	YES	1	NO	**
MP1DN	M-JPEG, H264 C-mount camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	**
MP2DN	M-JPEG, H264 C-mount camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	**
MP3DN	M-JPEG, H264 C-mount camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	**
MP5DN	M-JPEG, H264 C-mount camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	2	NO	**
MP8P	M-JPEG, 4CH dome camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	4	NO	**
MP8D	M-JPEG, 4CH dome camera	N/A	N/A	N/A	N/A	YES	YES	N/A	YES	4	NO	**
ZN-PT304WL	MPEG4 PTZ indoor camera	N/A	N/A	YES	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
ZN-PT304L	MPEG4 PTZ camera	N/A	N/A	YES	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
ZN-D2024	MPEG4 dome camera	1x	1x	N/A	N/A	YES	YES	N/A	YES	2	NO	by I.E.
ZVS306	MPEG4 videoseve	1x	1x	YES	YES	YES	YES	N/A	YES	2	NO	by I.E.
ZN-YH305	MPEG4 CS-mount camera	1x	N/A	N/A	N/A	N/A	YES	N/A	YES	1	NO	by I.E.
DDK1500	MPEG4 dome & CS-mount camera	1x	1x	N/A	YES	YES	YES	N/A	YES	2	NO	by I.E.
C-NV4VS	MPEG4 4CH videoserver	N/A	N/A	N/A	N/A	N/A	YES	N/A	YES	4	NO	by Specific application
ZR-DHC1630NP	MPEG4 DVR	16x	N/A	YES	N/A	YES	YES	YES	YES	16	NO	TBI
ZR-DHC830NP	MPEG4 DVR	8x	N/A	YES	N/A	YES	YES	YES	YES	8	NO	TBI
ZR-DHC3240	MPEG4 DVR	16	16	YES	N/A	YES	YES	YES	YES	32	NO	**
DR4N-DVD	MPEG4 DVR	4x	1x	YES	N/A	YES	YES	YES	YES	4	NO	TBI
DR8N-DVD	MPEG4 DVR	8x	8x	YES	N/A	YES	YES	YES	YES	8	NO	TBI
DR16N-DVD	MPEG4 DVR	16x	16x	YES	N/A	YES	YES	YES	YES	16	NO	TBI
DR4H-DVD	4CH H.264 DVR	4	1	YES	N/A	YES	YES	YES	YES	4	NO	**
DR8H-DVD	8CH H.264 DVR	8	8	YES	N/A	YES	YES	YES	YES	8	NO	**
DR16H-DVD	16CH H.264 DVR	16	16	YES	N/A	YES	YES	YES	YES	16	NO	**
DR4H-Lite	H.264 DVR	4	N/A	YES	N/A	N/A	YES	YES	YES	4	NO	**
DR8NRT	MPEG4 DVR	8x	8x	YES	N/A	YES	YES	YES	YES	8	NO	TBI
DR16NRT	MPEG4 DVR	16x	16x	YES	N/A	YES	YES	YES	YES	16	NO	TBI
ZN-D100VPE	H.264, MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-DT350VPE	H.264, MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-DNT350VPE	H.264, MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.

Device Model	Device Type	Alarm Inputs	Alarm Outputs	Direct PTZ	Transparent PTZ	Motion Detector	NVR Recording	DVR Recording/Playback	Videowall Live Display	Encoders	Audio	Remote Config
ZN-DWNT350VPE	H.264, MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-D310APE	MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-DT350APE	MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-DNT350APE	MPEG4, MJPEG dome camera	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-Y11VPE	H.264, MPEG4, MJPEG CS mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-NH11VPE	H.264, MPEG4, MJPEG CS mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-NHW11VPE	H.264, MPEG4, MJPEG CS mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-NH21VPE	H.264, MPEG4, MJPEG CS mount camera	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-S100V	H.264 videosever	1x	1x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-S1000VE	H.264 videosever	2x	2x	YES	YES	YES	YES	N/A	YES	2	YES	by I.E.
ZN-S100AE	MPEG4 videosever	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-S1000AE	MPEG4 videosever	1x	1x	YES	YES	YES	YES	N/A	YES	1	YES	by I.E.
ZN-S4000AE	MPEG4 4CH videosever	4x	4x	YES	YES	YES	YES	N/A	YES	4	YES	by I.E.
PixelPro ZN-C1	H.264 D1 CS-mount camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
PixelPro ZN-C1M	H.264 720p CS-mount camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
PixelPro ZN-C2M	H.264 1080p CS-mount camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
PixelPro ZN-DT1A	H.264 D1 minidome camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
PixelPro ZN-DT1MA	H.264 720p minidome camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
PixelPro ZN-DT2MA	H.264 1080p minidome camera	1x	1x	NO	NO	YES	YES	N/A	YES	2	YES	by I.E.
ZN-PT-IP	H264 camera	1x	1x	YES	NO	NO	YES	N/A	YES	2	NO	by I.E.
VSolP Videowall	VSolP Video-wall v3.0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
VSolP Videowall2	VSolP Video-wall v3.1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

** configured when adding device to VSolP Lite

Transparent PTZ protocols:	All-View Serial All-View V3 Serial BBV Serial C-Dome Serial GANZ-PT Serial	Pelco D Serial Pelco P Serial Sensormatic Serial Vicon Serial
All protocols implement:	Zoom, Pan, Tilt Presets store recall Presets renaming	OSD (when supported) Tours (when supported)

Appendix C – Specific Device Considerations

This chapter contains the following information:

- Adding ZV-S306 and ZN-D2024 Devices to VSoIP Lite
- Adding DRH-DVD and DR4H Lite DVRs

Adding ZV-S306 and ZN-D2024 Devices to VSoIP Lite

If you are adding a Ganz ZV-S306 or ZN-D2024 camera to the site, please note that these device types require careful configuration to ensure that VSoIP Lite receives event information from them.

These cameras have two ports, primary and secondary, which are available for connections. These ports must be configured on the camera itself.

When adding one of these devices to VSoIP Lite, you must enter the IP address followed by the primary port number, for example: 192.169.1.21:80 (where the device IP address is 192.168.1.21 and the primary port is 80).

Once the device has been added, VSoIP Lite queries it using the primary port to determine the secondary port number.

VSoIP Lite then establishes a connection to the secondary port. This allows VSoIP Lite to receive live event information, e.g. Motion Detection events.

Caution: If the secondary port number is a “well known” HTTP port for example 80 or 8080 it may be unduly affected by firewall and anti-virus software. This may prevent event information being received by VSoIP Lite.

To avoid this, please ensure that no firewall or anti-virus software is running on the same platform as the server. Alternatively, ensure that the device’s secondary port is configured to something other than a well known HTTP port.

Adding DRH-DVD and DR4H Lite DVRs

VSoIP Lite allows the following ports to be specified for these DVR types when adding/configuring the device to the site:

- RTSP_PORT: the RTSP port used for live and playback services. This port number should be appended to the IP address for the device, as follows:

<IP_ADDRESS>:<PORT>

Caution: The default RTSP port number is 554. This number should not be changed or recording playback will not function correctly.

- ADVANCED_PORT: the port used for advanced services such as alarm notification and PTZ. This port number should be specified in the Configuration Port field.

Index

A

- acknowledging alarms 41
- activating
 - PTZ support 37
 - triggers 27
- adding
 - devices, manually 21
 - devices, using autodiscovery 19
- adding devices 19
- alarms
 - acknowledging 41
 - closing 42
 - viewing properties 40
- application does not start 17
- aspect ratio, default setting 58
- audio
 - listening to 30
 - timeout 31
- audit trail 43
- autodiscovery 19

C

- camera sequences
 - configuring 31
 - deleting 31
 - editing 31
- cameras
 - displaying title 59
 - ZV-S306 21
- changing
 - device names 26
 - sequences 31
- checking connectivity 66
- closing alarms 42
- command prompt, opening 60
- computer's IP address, determining 60
- configuring
 - devices 19
 - devices using web interface 24
 - PTZ 28
 - sequences 31
 - stream settings 7
 - triggers 27
 - video sources 26
- controlling PTZ cameras 37
- controls, live view 32
- CPU usage, maximum 58
- creating
 - recordings 44
 - sequences 31

D

- default
 - playback offset time 58
- deleting
 - devices 25
 - recordings 53
 - sequences 31

- deleting recordings 53
- devices
 - adding 19
 - adding manually 21
 - adding using autodiscovery 19
 - autodiscovery 19
 - changing names 26
 - configuration 19
 - deleting 25
 - grouping 22
 - specifying location 22
 - using web interface for configuration 24
- DHCP, use of 12
- Direct-3D hardware support 13
- disabling
 - logging 69
- disabling TCP/IPv6 19
- displaying
 - camera title 59
 - recordings 48

E

- editing
 - sequences 31
- enabling logging 68
- exported recordings 55
- exporting
 - recordings 55

F

- factory defaults, restoring 56
- feedback
 - preventing 31
- firewalls 12
- and web device configuration 24

G

- grouping devices 22

I

- inactivity timeout, default setting 58
- installation procedure 14
- installing
 - Player application 55
- IP addresses
 - determining 60
 - DHCP 12

L

- layouts
 - specifying 33
- listening to audio 30
- listing recordings 50
- live video
 - controls 32
 - snapshots 36
 - starting 34
 - stopping 34
- location text 22
- logging
 - disabling 69
 - enabling 68

M

- main menu 33
- manual device addition 21
- Microsoft Direct-X 9.0c 13
- moving PTZ cameras 37

N

- networking settings 12
- NVR
 - sampling 46

O

- opening
 - command prompt 60
 - run dialog 60
- operating system 11
- overview
 - system 6

P

- pane layout 33
- Pan-Tilt-Zoom
 - configuration 28
- password
 - changing 18
 - expiry, default 58
 - history count, default 58
 - reminder, default 58
- persisted layout, loading 59
- ping command, using 67
- playback offset time default 58
- Player application
 - installation 55
- Player application, installation 55
- playing back recordings 50
- port numbers, specifying 21
- port usage 12
- precautions, when shutting down 9
- pre-installation
 - VSolP Lite 12
- preventing feedback 31
- previous layout, displaying 59
- PTZ cameras
 - control 37
 - moving and zooming 37
 - timeout, default 58
- PTZ configuration 28
- PTZ support, activating 37

R

- recording footage
 - synchronising 54
- recordings
 - creating 44
 - deleting 53
 - displaying 48
 - exporting 55
 - listing 50
 - playing back 50
 - storage 44
 - taking snapshot 52
- requirements
 - additional software 11
 - operating system 11
 - UPS 11
- restoring factory defaults 56
- run dialog, opening 60

S

- sampling, streams 46
- security software 13
- sequences 38
 - configuring 31
 - deleting 31
 - editing 31
- shutting down PC, precautions 9
- snapshots
 - default location 58
 - live video 36
 - recorded video 52
- specifying
 - location 22
 - pane layout 33
 - port numbers 21
- starting up
 - live video 34
- stopping
 - live video 34
- storing recordings 44
- stream sampling 46
- stream settings, configuring 7
- streams
 - increasing number 14
- supported devices 71
- synchronising recording footage 54
- system
 - components 6
 - information, viewing 57
 - overview 6

T

- taking snapshots
 - live video 36
 - recorded video 52
- TCP/IPv6, disabling 19
- timeout, audio 31
- triggers, configuring 27
- troubleshooting
 - web configuration access 24
- troubleshooting, application does not start 17

U

- uninterruptable power supply 11
- upgrading streams 14
- user overview 18
- users
 - changing passwords 18
- using sequences 38

V

- video pane layout 33
- video sources, configuring 26
- viewing
 - alarm properties 40
 - system information 57

W

- watermark, default 58
- web device configuration,
 - troubleshooting 24
- Windows Events Viewer 62
- Windows Services 65

Z

- zooming PTZ 37
- ZV-S306 cameras 21

